ISACA®
Trust in, and value from, information systems

COBIT® 5

para Seguridad de la Información

COBIT® 5
AN ISACA® FRAMEWORK

ISACA®
Con más de 100.000 asociados en 180 países, ISACA (*www.isaca.org*) es un líder global proveedor de conocimiento, certificaciones, comunidad, promoción y educación sobre aseguramiento y seguridad de sistemas de información (SSII), gobierno empresarial y gestión de TI y riesgo relacionado con TI y cumplimiento. Fundada en 1969, ISACA, independiente y sin ánimo de lucro, celebra conferencias internaciones, publica el *ISACA® Journal* y desarrolla estándares internaciones de control y auditoría de SSII, que ayudan a sus miembros a asegurar la confianza en, y aportar valor desde, los sistemas de información. También avanza y avala habilidades y conocimientos en TI mediante los globalmente reconocidos certificados (CISA®) Certified Information Systems Auditor®, (CISM®) Certified Information Security Manager®, (CGEIT®) Certified in the Governance of Enterprise IT® y (CRISC™) Certified in Risk and Information Systems Control™.

ISACA actualiza continuamente el marco de referencia COBIT®, el cual ayuda a los profesionales de TI y líderes de las organizaciones a llevar a cabo sus responsabilidades en la gestión y gobierno de TI, particularmente en las áreas de aseguramiento, seguridad, riesgo y control y proporcionar valor al negocio.

Disclaimer
ISACA has designed this publication, *COBIT® 5 for Information Security* (the 'Work'), primarily as an educational resource for security professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, security professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Renuncia
ISACA ha designado esta publicación *COBIT® 5 para Seguridad de la Información* (el 'Trabajo'), principalmente como un recurso educativo para los profesionales de la seguridad. ISACA no pretende que el uso del Trabajo asegure el éxito del resultado. No debe considerarse que el Trabajo incluye toda la información adecuada, procedimientos y pruebas o excluye otra información, procedimientos, pruebas que están razonablemente dirigidas a obtener el mismo resultado. Para determinar la propiedad de cualquier información específica, procedimiento o prueba, los profesionales de la seguridad deberían aplicar su propio juicio profesional a las circunstancias especificas presentadas por cada sistema particular o entorno de tecnologías de la información.

Quality Statement
This Work is translated into Spanish from the English language version of *COBIT® 5 for Information Security* by the ISACA® Madrid Chapter with the permission of ISACA®. The ISACA® Madrid Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

Declaración de Calidad
Este Trabajo ha sido traducido al español desde la versión en inglés de *COBIT® 5 para Seguridad de la Información* por el Capítulo de Madrid de ISACA® con permiso de ISACA®. El capítulo de ISACA® Madrid asume responsabilidad única por la exactitud y la fidelidad de la traducción

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE.UU.
Teléfono: +1.847.253.1545
Fax: +1.847.253.1443
Email: *info@isaca.org*
Página Web: *www.isaca.org*

Comentarios: *www.isaca.org/cobit*
Participar en el Centro de Conocimiento de ISACA: *www.isaca.org/knowledge-center*
Sigue a ISACA en Twitter: *https://twitter.com/ISACANews*
Únete a la conversación COBIT en Twitter: #COBIT
Únete a ISACA en LinkedIn: ISACA (Oficial), , *http://linkd.in/ISACAOfficial*
Me gusta ISACA en Facebook: *www.facebook.com/ISACAHQ*

COBIT® 5 para Seguridad de la Información
ISBN 978-1-60420-454-4
Impreso en los Estados Unidos
3

RECONOCIMIENTOS

ISACA quiere reconocer la labor de:

Fuerza de trabajo de COBIT 5 para Seguridad de la Información
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Grecia, Presidente
Manuel Aceves Mercenario, CISA, CISM, CGEIT, CRISC, CISSP, FCITSM, Cerberian Consulting, S.A. de C.V., México
Mark Chaplin, Information Security Forum, Reino Unido
Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, EE.UU.
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia
Rolf M. von Roessing, CISA, CISM, CGEIT, CISSP, FBCI, Forfa AG, Suiza

Equipo de Desarrollo
Floris Ampe, CISA, CGEIT, CRISC, CIA, ISO 27000, PwC, Bélgica
Stefanie Grijp, PwC, Bélgica
Ariel Litvin, CRISC, CCSK, PwC, Israel
Bart Peeters, CISA, PwC, Bélgica
Christopher Wilken, CISA, CGEIT, PwC, EE.UU.

Participantes de Talleres
Elisabeth Judit Antonsson, CISM, Nordea Bank, Suecia
Garry Barnes, CISA, CISM, CGEIT, CRISC, Stratsec, Australia
Todd Fitzgerald, CISA, CISM, CGEIT, CRISC, CISSP, PMP, ManpowerGroup, EE.UU.
Erik P. Friebolin, CISA, CISM, CRISC, CISSP, ITIL, PCI-QSA, EE.UU.
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, ITIL, 6 Sigma, Quest Software, España
Roger Gallego, Entelgy Consulting S.A., España
Norman Kromberg, CISA, CGEIT, CRISC, CQA, NBE, Alliance Data, EE.UU.
Aureo Monteiro Tavares da Silva, CISM, CGEIT, Pelissari, Brasil
Naiden Nedelchev, Ph.D., CISM, CGEIT, CEH, ITIL V2 Manager, Mobiltel EAD, Bulgaria
Steve Orrin, Intel Corp., EE.UU.
Christian Palomino, CISA, CISM, CGEIT, Melia Hotels International, España
Vernon Richard Poole, CISM, CGEIT, CRISC, Sapphire, Reino Unido
Jeffrey Roth, CISA, CGEIT, CISSP, Parsons, EE.UU.
Craig Silverthorne, CISA, CISM, CGEIT, CRISC, CPA, IBM Global Business Services, EE.UU.
Cathie Skoog, CISM, CGEIT, CRISC, IBM, EE.UU.
Robert E. Stroud, CGEIT, CRISC, CA Technologies, EE.UU.
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Bélgica
Mike Villegas, CISA, CEH, CISSP, GSEC, Newegg, Inc., EE.UU.

Revisores Expertos
Sanjiv Agarwala, CISA, CISM, CGEIT, CISSP, ITIL, MBCI, Oxygen Consulting Services Pvt. Ltd., India
Jean-Luc Allard, CISA, CISM, MISIS scri, Bélgica
Elisabeth Judit Antonsson, CISM, Nordea Bank, Suecia
Garry Barnes, CISA, CISM, CGEIT,ww CRISC, Stratsec, Australia
Allan Boardman, CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, Reino Unido
Jeimy J. Cano, Ph.D., CFE, CMAS, Ecopetrol S.A, Colombia
Cilliam Cuadra, CISA, CISM, CRISC, Banco Nacional de Costa Rica, Costa Rica
Erick Dahan, CISA, CISM, CISSP, PSP Investments, Canadá
Heidi L. Erchinger, CISA, CRISC, CISSP, System Security Solutions Inc., EE.UU.
Todd Fitzgerald, CISA, CISM, CGEIT, CRISC, CISSP, PMP, ManpowerGroup, EE.UU.
Erik P. Friebolin, CISA, CISM, CRISC, CISSP, ITIL, PCI-QSA, EE.UU.
Joerg Fritsch, CISM, CRISC, NATO, Países Bajos
Timothy M. Grace, CISA, CISM, CRISC, CIA, MorganFranklin Corp., EE.UU.
Jimmy Heschl, CISA, CISM, CGEIT, ITIL Expert, bwin.party digital entertainment plc, Austria
Jerry M. Kathingo, CISM, Infosec Consulting Company, Kenia
Luc Kordel, CISA, CISM, CISSP, CIA, RFA, Belfius Bank, Bélgica
Kyeong Hee Oh, CISA, CISM, Fullbitsoft, Corea
Gary Langham, CISA, CISM, CGEIT, CISSP, CPFA, Australia
Yves Le Roux, CISM, CISSP, CA Technologies, Francia

RECONOCIMIENTOS *(CONT.)*

Revisores Expertos (cont.)
Oscar Mauricio Moreno Lopez, CISA, CISM, CGEIT, CISSP, ITIL(f), F&M Technology, Colombia
Tamanu Lowkie, CISM, CAP, CISSP, PMP, EE.UU.
Aureo Monteiro Tavares da Silva, CISM, CGEIT, Pelissari, Brasil
Naiden Nedelchev, Ph.D., CISM, CGEIT, CEH, ITIL V2 Manager, Mobiltel EAD, Bulgaria
Hitoshi Ota, CISA, CISM, CGEIT, CRISC, CIA, Mizuho Corporate Bank, Japón
Christian Palomino, CISA, CISM, CGEIT, Melia Hotels International, España
Maria Patricia Prandini, CISA, CRISC, Universidad de Buenos Aires, Argentina
Abdul Rafeq, CISA, CGEIT, CIA, FCA, A. Rafeq & Associates, India
R.V. Ramani, CISM, CGEIT, Paramount Computer Systems, Emirates Árabes Unidos
Jeffrey Roth, CISA, CGEIT, CISSP, Parsons, EE.UU.
Cheryl Santor, CISSP, CNA, CNE, Metropolitan Water District of SoCal, EE.UU.
Tim Sattler, CISA, CISM, CRISC, CCSK, CISSP, Jungheinrich AG, Alemania
Gurvinder Pal Singh, CISA, CISM, CRISC, Australia
Jonathan D. Sternberg, CISA, CISM, CRISC, CISSP, FFSI, FLMI, Northwestern Mutual, EE.UU.
John G. Tannahill, CISM, CGEIT, CRISC, CA, John Tannahill & Associates, Canadá
Darlene Tester, JD, CISM, CHSS, CISSP, Bluestem Brands Inc., EE.UU.
Smita Totade, Ph.D., CISA, CISM, CGEIT, CRISC, FIEI, National Insurance Academy, India
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Bélgica
Bruce R. Wilkins, CISA, CISM, CGEIT, CRISC, CISSP, TWM Associates, Inc., EE.UU.
Hui Zhu, CISA, CISM, CGEIT, BlueImpact, Canadá

Equipo de Traducción ISACA Madrid
Mª Teresa Avelino Carmona, CISA, CISSP, PMP, España
Alberto Benavente Martínez CISSP, ISO20000 Lead Auditor, Director Seguridad (Ministerio Interior) IBM Global Services, España
María José Carmona Carmona, CISA, CRISC, Mediaset, España
José Fernando Carvajal-Vión, CISA, CISM, CISSP, CGEIT, CRISK, ISO 27001 Lead Auditor, ITIL(f), España
María Jesús Casado, CISA, CGEIT, CDPP, Intervención General de la AGE, España
Joaquín Castillón Colomina, CISA, CGEIT, ISO 27001 LA, ISO 22301 LA, ITIL(f), EY, España
Oliver Crespo, CISA,CISM, Grupo Generali España, España
Iván de Antonio Tejado, CISA, CISM, CISSP, ISO 27001 Lead Auditor, PMP, ITIL(f), España
David Echarri Santamaría, CISA, ITIL(f), España
Jerónimo Escalante, ITIL, ASQ Process Improvement Associate, Cast-Info, España
Ana Belén, Galán López, CISA, CISM,CRISC,ISO27001 LA,ISO22301 LA, Bankinter, España
Miguel Garcia-Menendez, CGEIT, CISM, CISA, CRISC, iTTi – Innovation & Technology Trends Institute, España
Fernando Gómez-Alfonso, CISA, Hécate Proyectos, España
Luis Francisco González Hernández, CISA, España
Daniel Largacha Lamela, CISA, MAPFRE, España
Rafael Martínez Ranera, CISA, CISM,ISO27001 LA, España
Juan Manuel Matalobos, CISA, CISM, CRISC, CISSP, España
Jorge Álvaro Navas Elorza, CISA, ISO 27001 Lead Auditor, Intervención General de la Administración del Estado (IGAE), España
Irene Palacios Herranz, CISA, ENDESA. – Enel Group, España
Javier Palomares, CISA, CRISC, Hotelbeds, España
Christian Palomino Herrero, CISA, CISM, CGEIT, Meliá Hotels International, España
Pablo Pastor Mediavilla, CISA, FUJITSU TECHNOLOGY SOLUTIONS, España
Javier Pérez Abad, CISA, CISM, España
Fernando Puerto Mendoza, CISA, España
Susana Quiroga Chávez, CISA, Pfizer, España
Dr. José Ramón Coz, CRISC, CISA, CISM, CGEIT, COBITf, PRINCE2p, MSPp, TOGAF, ITIL(f), ISDEFE, España
Antonio Ramos, CISA, CISM, CGEIT, Leet Security & n+1 Intelligence & Research España
Adolfo Ranero Serrano, CISA, CRISC, VASS, España
Luis Fernando Real Martín, España
Eduardo Rodríguez Ringach, CGEIT, CRISC, TOGAF, España
José Manuel Román Fernández-Checa, CISA, CISSP, ITIL (f), España
Ana Sabio Faraldo, CIA, NH Hoteles, España
Julio Sánchez Fernández, CISM, CISA, CRISC, CGEIT, Director Seguridad (Ministerio Interior), Sociedad Estatal Loterías y Apuestas del Estado, S.A. (SELAE), España

RECONOCIMIENTOS *(CONT.)*

Equipo de Traducción ISACA Madrid (cont.)
Luis Enrique Sánchez Crespo, CISA, ISO27001 Leader Auditor, Sicaman Nuevas Tecnologías, España
Iván Sánchez López, CISA, CISM, CISSP, ISO27001 Lead Auditor, ITIL(f). Vodafone Group, Alemania
Mª Jesús Sanz Navalpotro, MSc,CISA,CISM,ISO27001LA,ITIL(f)., Indra Sistemas, España
Juan Antonio Tercero López, CISM, Novo Nordisk Pharma, España
Juan Carlos Torres Cañete, CISM, CRISC, Accenture, España
Miguel Tubía Angulo, CISA, ITIL(f)., ITIL SS., Specialist Computer Centres, España
Zulayka Vera, CISA, CISM, CRISC, CGEIT, PCI QSA, ISO 27001 Lead Aud., CDPP, PCIP, ITIL(f)., IBM Global Services, España
Juan Carlos Vigo, CISA, CRISC, CGEIT, Everis, España
Joris Vredeling, ISACA Madrid, España

Consejo de Administración de ISACA
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retirado), EE.UU., Presidente Internacional
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Grecia, Vice Presidente
Gregory T. Grocholski, CISA, The Dow Chemical Co., EE.UU., Vice Presidente
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Vice Presidente
Niraj Kapasi, CISA, Kapasi Bangad Tech Consulting Pvt. Ltd., India, Vice Presidente
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management, Inc., EE.UU., Vice Presidente
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia, Vice Presidente
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd. (retirado), EE.UU., ex Presidente Internacional
Lynn C. Lawton, CISA, CRISC, FBCS CITP, FCA, FIIA, KPMG Ltd., Russian Federation, ex Presidente Internacional
Allan Neville Boardman, CISA, CISM, CGEIT, CRISC, CA (SA), CISSP, Morgan Stanley, GB, Director
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Bélgica, Director

Junta de Expertos
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Bélgica, Presidente
Michael A. Berardi Jr., CISA, CGEIT, Bank of America, EE.UU.
John Ho Chi, CISA, CISM, CRISC, CBCP, CFE, Ernst & Young LLP, Singapur
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, EE.UU.
Jon Singleton, CISA, FCA, Auditor General of Manitoba (retirado), Canadá
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, Francia

Comité Marco (2009-2012)
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, Francia, Presidente
Steven A. Babb, CGEIT, CRISC, Betfair, Reino Unido
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Sergio Fleginsky, CISA, Akzo Nobel, Uruguay
John W. Lainhart, IV, CISA, CISM, CGEIT, CRISC, IBM Global Business Services, EE.UU.
Anthony P. Noble, CISA, CCP, Viacom, EE.UU.
Derek J. Oliver, Ph.D., DBA, CISA, CISM, CRISC, CITP, FBCS, FISM, MInstISP,
Ravenswood Consultants Ltd., Reino Unido
Rolf M. von Roessing, CISA, CISM, CGEIT, CISSP, FBCI, Forfa AG, Suiza

Afiliados y patrocinadores de ISACA e Instituto para el Gobierno de TI® (ITGI®)
Information Security Forum
Institute of Management Accountants Inc.
Capítulos de ISACA
ITGI Francia
ITGI Japón
Norwich University
Socitum Performance Management Group
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School

ASIS International
Hewlett-Packard
IBM
Symantec Corp.
TruArx Inc.

Página dejada en blanco intencionadamente

Tabla de Contenidos

Lista de Figuras 11

Resumen Ejecutivo 13
Introducción 13
Motivos 13
Beneficios 15
Público Objetivo 16
Convenciones Utilizadas y Resumen 16

Sección I. Seguridad de la Información 19
Capítulo 1. Definición de Seguridad de la Información 19

Capítulo 2. Principios de Cobit 5 21
2.1 Visión General 21
2.2 Principio 1. Satisfacer las Necesidades de las Partes Interesadas 21
2.3 Principio 2. Cubrir la Empresa Extremo-a-Extremo 22
2.4 Principio 3. Aplicar un Marco de Referencia Único Integrado 22
2.5 Principio 4: Hacer Posible un Enfoque Holístico 23
2.6 Principio 5. Separar el Gobierno de la Gestión 23

Sección II. Uso de los Catalizadores de Cobit 5 para Implantar la Seguridad de la Información en la Práctica 25
Capítulo 1. Introducción 25
1.1 El modelo genérico de catalizadores 25
1.2 Gestión del Rendimiento de los Catalizadores 26
1.3 *COBIT 5 para Seguridad de la información* y los Catalizadores 26

Capítulo 2. Catalizador: Principios, Políticas y Marcos de Referencia 27
2.1 Principles, Policies and Framework Model 27
2.2 Principios de Seguridad de la Información 29
2.3 Políticas de Seguridad de la Información 29
2.4 Adaptar las Políticas al Entorno de la Empresa 30
2.5 Ciclo de Vida de las Políticas 31

Capítulo 3. Catalizador: Procesos 33
3.1 El Modelo de Procesos 33
3.2 Procesos de Gobierno y Gestión 34
3.3 Procesos de Gobierno y Gestión de Seguridad de la Información 34
3.4 Relación de los Procesos con otros Catalizadores 35

Capítulo 4. Catalizador: Estructuras Organizativas 37
4.1 Modelo de Estructuras Organizativas 37
4.2 Roles y Estructuras de Seguridad de la Información 38
4.3 Responsabilidad Sobre la Seguridad de la Información 39

Capítulo 5. Catalizadores: Cultura, Ética y Comportamiento 41
5.1 Modelo Cultural 41
5.2 Ciclo de Vida de la Cultura 42
5.3 Líderes y Campeones 42
5.4 Comportamiento Deseable 43

Capítulo 6. Catalizador: Información 45
6.1 Modelo de Información 45
6.2 Tipos de Información 46
6.3 Grupos de interés en la Información 46
6.4 Ciclo de Vida de la Información 47

Capítulo 7. Catalizador: Servicios, Infraestructuras y Aplicaciones 49
7.1 Modelo de Servicios, Infraestructuras y Aplicaciones 49
7.2 Servicios, Infraestructuras y Aplicaciones de Seguridad de la Información 50

Capítulo 8. Catalizador: Personas, Habilidades y Competencias 51
8.1 Modelo de Personas, Habilidades y Competencias 51
8.2 Habilidades y Competencias Relacionadas con la Seguridad de la Información 52

Sección III. Adaptando *COBIT 5 para SegurIdad de la InformacIón* al Entorno de la Empresa 53
Capítulo 1. Introducción 53

Capítulo 2. Implementación de Iniciativas de Seguridad de la Información 55
2.1. Considerando el Contexto Empresarial de la Seguridad de la Información 55
2.2. Creando el Entorno Apropiado 55
2.3. Reconociendo Puntos Débiles y Eventos Desencadenantes 56
2.4. Posibilitar el Cambio 56
2.5. Un Enfoque del Ciclo de Vida 57

Capítulo 3. Usando *COBIT 5 para SegurIdad de la InformacIón* para Conectar otros Marcos de Trabajo, Modelos, Buenas Prácticas y Estándares 59

Apéndices
Apéndice A. Guia Detallada: Catalizador de Principios, Políticas y Marcos 61
A.1 Principios de la Seguridad de la Información 61
A.2 Política de Seguridad de la Información 63
A.3 Políticas Específicas de Seguridad de la Información Dirigidas por la Función de Seguridad de la Información 63
A.4 Políticas Específicas de Seguridad de la Información Dirigidas por Otras Funciones Dentro de la Empresa 65

Apéndice B. Guía Detallada: Catalizador de Procesos 67
B.1 Evaluar, Orientar y Supervisar (EDM) 69
B.2 Alinear, Planificar y Organizar (APO) 81
B.3 Construir, Adquirir e Implementar (BAI) 115
B.4 Entrega, Servicio y Soporte (DSS) 141
B.5 Supervisar, Evaluar y Valorar (MEA) 159

Apéndice C. Guía Detallada: Catalizador de Estructuras Organizativas 169
C.1 Director de Seguridad de la Información (CISO) 169
C.2 Comité de Dirección de Seguridad de la Información 171
C.3 Gerente de Seguridad de la Información (ISM) 172
C.4 Comité de Gestión de Riesgo Empresarial 174
C.5 Custodios de la Información/Propietarios de Negocio 174

Apéndice D. Guía Detallada: Catalizador de Cultura, Ética y Comportamiento 175
D.1 Comportamientos 175
D.2 Liderazgo 176

Apéndice E. Guía Detallada: Catalizador de Información 179
E.1 Plantilla para las Partes Interesadas de la Seguridad de la Información 179
E.2 Estrategia de Seguridad de la Información 181
E.3 Presupuesto de Seguridad de la Información 182
E.4 Plan de Seguridad de la Información 183
E.5 Políticas 184
E.6 Requerimientos de Seguridad de la Información 184
E.7 Material de Concienciación 184
E.8 Informes de Revisión de la Seguridad de la Información 185
E.9 Cuadro de Mando de la Seguridad de la Información 186

Apéndice F. Guía Detallada: Catalizador de Servicios, Infraestructura y Aplicaciones 189
F.1 Arquitectura de Seguridad 189
F.2 Concienciación en Seguridad 191
F.3 Desarrollo Seguro 192
F.4 Evaluaciones de Seguridad 192
F.5 Sistemas Adecuadamente Asegurados y Configurados, en Línea con los Requerimientos y la Arquitectura de Seguridad 193
F.6 Acceso de Usuario y Derechos de Acceso de Acuerdo con los Requerimientos del Negocio 194
F.7 Protección Adecuada Frente a Software Malicioso (*Malware*), Ataques Externos e Intentos de Intrusión 196
F.8 Respuesta a Incidentes Adecuada 197
F.9 Pruebas de Seguridad 198
F.10 Servicios de Monitorización y Alerta para Eventos relacionados con la Seguridad 199

Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias 201
G.1 Gobierno de la Seguridad de la Información 201
G.2 Formulación de la Estrategia de Seguridad de la Información 202
G.3 Gestión de Riesgos de Seguridad de la Información 203
G.4 Desarrollo de la Arquitectura de Seguridad de la Información 203
G.5 Operaciones de Seguridad de la Información 204
G.6 Evaluación, Pruebas y Cumplimiento de la Información 205

Apéndice H. Mapeos Detallados 207

Acrónimos 215

Glosario 217

Página dejada en blanco intencionadamente

Lista de Figuras

Figura 1—Familia de Productos COBIT 5 ... 13
Figura 2—COBIT 5 y su Relación con la Seguridad de la Información ... 14
Figura 3—*Capacidades COBIT 5 para de Seguridad de la Información* ... 16
Figura 4—Principios de COBIT 5 ... 21
Figura 5—Visión General de la Cascada de Metas de COBIT 5 ... 22
Figura 6—Catalizador de COBIT 5: Modelo Sistémico con Interactuación de Catalizadores ... 23
Figura 7—Modelo de Referencia de Procesos de COBIT 5 ... 24
Figura 8—Catalizadores COBIT 5: Genéricos ... 25
Figura 9—Catalizador de COBIT 5: Principios, Políticas y Marcos de Referencia ... 27
Figura 10—Marco de Políticas ... 28
Figura 11—Catalizador de Cobit 5: Proceso ... 33
Figura 12—Catalizador de COBIT 5: Estructuras Organizativa ... 37
Figura 13—Roles/Estructuras Específicas de Seguridad de la Información ... 38
Figura 14—Ventajas y Desventajas de Posibles Caminos para el Reporte sobre la Seguridad de la Información ... 39
Figura 15—Catalizador COBIT 5: Cultura, Ética y Comportamiento ... 41
Figura 16—Catalizador de COBIT 5: Información ... 45
Figura 17—Ejemplos de Grupos de Interés para Información Relacionada con Seguridad de la Información (Empresas Pequeñas /Medianas) ... 47
Figura 18—Catalizador COBIT 5: Servicios, Infraestructuras y Aplicaciones ... 49
Figura 19—Catalizador COBIT 5: Personas, habilidades y Competencias ... 51
Figura 20—Habilidades/Competencias de Seguridad de la Información ... 52
Figura 21—Las Siete Fases de la Implementación del Ciclo de Vida ... 57
Figura 22—Principios para la Seguridad de la Información ... 61
Figura 23—Políticas Específicas de Seguridad de la Información Dirigidas por Otras Funciones Dentro de la Organización: Alcance ... 65
Figura 24—Modelo de Referencia de Procesos de COBIT 5 ... 67
Figura 25—CISO: Mandato, Principios Operativos, Ámbito de Control y Nivel de Autoridad ... 169
Figura 26—CISO: Matriz RACI a Alto Nivel con Prácticas Clave ... 170
Figura 27—CISO: Entradas y Salidas ... 170
Figura 28—ISSC: Composición ... 171
Figura 29—ISSC: Mandato, Principios Operativos, Ámbito de Control y Nivel de Autoridad ... 171
Figura 30—ISSC: Matriz RACI a Alto Nivel ... 172
Figura 31—ISSC: Entradas y Salidas ... 172
Figura 32—ISM: Mandato, Principios Operativos, Ámbito de Control y Nivel de Autoridad ... 172
Figura 33—ISM: Matriz RACI de Alto Nivel ... 173
Figura 34—ISM: Entradas y Salidas ... 173
Figura 35—Comité de ERM: Composición ... 174
Figura 36—Comité de ERM: Matriz RACI de Alto Nivel ... 174
Figura 37—Custodios de la Información/Propietarios de Negocio: Matriz RACI de Alto Nivel ... 174
Figura 38—Plantilla de Información Relacionada con Partes Interesadas para la Seguridad de la Información ... 180
Figura 39—Planificación de los Servicios: Descripción de la Capacidad del Servicio ... 189
Figura 40—Planificación de los Servicios: Atributos ... 190
Figura 41—Planificación de los Servicios: Objetivos ... 190
Figura 42—Servicios de Concienciación en Seguridad: Descripción de la Capacidad del Servicio ... 191
Figura 43—Servicios de Concienciación en Seguridad: Atributos ... 191
Figura 44—Servicios de Concienciación en Seguridad: Objetivos ... 191
Figura 45—Servicios de Desarrollo Seguro: Descripción de la Capacidad del Servicio ... 192
Figura 46—Servicios de Desarrollo Seguro: Atributos ... 192
Figura 47—Servicios de Desarrollo Seguro: Objetivos ... 192
Figura 48—Servicios de Evaluación de la Seguridad: Descripción de la Capacidad del Servicio ... 192
Figura 49—Servicios de Evaluación de la Seguridad: Atributos ... 193
Figura 50—Servicios de Evaluación de la Seguridad: Objetivos ... 193
Figura 51—Servicios de Sistemas Adecuadamente Asegurados: Descripción de la Capacidad del Servicio ... 193
Figura 52—Servicios de Sistemas Adecuadamente Asegurados: Atributos ... 194
Figura 53—Servicios de Sistemas Adecuadamente Asegurados: Objetivos ... 194
Figura 54—Servicios de Acceso de Usuario y Derechos de Acceso: Descripción de la Capacidad del Servicio ... 194
Figura 55—Acceso de Usuarios y Permisos de Acceso a los Servicios: Atributos ... 195

Figura 56—Servicios de Sistemas Adecuadamente Asegurados: Objetivos....196
Figura 57—Protección Contra Software Malicioso (Malware) y Ataques: Descripción de la Capacidad de Servicio....196
Figura 58—Protección Contra Software Malicioso (Malware) y Ataques: Atributos....197
Figura 59—Protección Contra Software Malicioso (Malware) y Ataques: Objetivos....197
Figura 60—Servicios de Respuesta a Incidentes: Descripción de la Capacidad de Servicio....197
Figura 61—Servicios de Respuesta a Incidentes: Atributos....198
Figura 62—Servicios de Respuesta a Incidentes: Objetivos....198
Figura 63—Servicios de Prueba de la Seguridad: Descripción de la Capacidad de Servicio....198
Figura 64—Servicios de Prueba de la Seguridad: Atributos....198
Figura 65—Servicios de Pruebas de Seguridad: Objetivos....199
Figura 66—Servicios de Monitorización y Mejora de la Seguridad de la Información: Descripción de la Capacidad de Servicio....199
Figura 67—Monitorizar y Mejorar los Servicios de la Seguridad de la Información: Atributos....199
Figura 68—Servicios de Monitorización y Mejora de la Seguridad de la Información: Objetivos....200
Figura 69—Gobierno de Seguridad de la Información: Experiencia, Educación y Cualificaciones....201
Figura 70—Gobierno de Seguridad de la Información: Conocimiento, Habilidades Técnicas y Habilidades en el Comportamiento....201
Figura 71—Formulación de la Estrategia de Seguridad de la Información: Experiencia, Formación y Cualificaciones....202
Figura 72—Formulación de la Estrategia de Seguridad de la Información: Conocimiento, Habilidades Técnicas y Habilidades en el Comportamiento....202
Figura 73—Formulación de la Estrategia de Seguridad de la Información: Roles/ Estructuras relacionados....202
Figura 74—Gestión de Riesgos de Información: Experiencia, Formación y Cualificaciones....203
Figura 75—Gestión de Riesgos de Información: Conocimiento, Habilidades Técnicas y Habilidades de Comportamiento....203
Figura 76—Desarrollo de la Arquitectura de Seguridad de la Información: Experiencia, Formación y Cualificaciones....203
Figura 77—Desarrollo de la Arquitectura de Seguridad de la Información: Conocimiento, Habilidades Técnicas y Habilidades de Comportamiento....204
Figura 78—Desarrollo de la Arquitectura de Seguridad de la Información: Rol/Estructura relacionada....204
Figura 79—Operaciones de Seguridad de la Información: Experiencia, formación y cualificaciones....204
Figura 80—Operaciones de Seguridad de la Información: Conocimiento, Habilidades Técnicas y Habilidades de Comportamiento....205
Figura 81—Operaciones de Seguridad de la Información: Rol/Estructura relacionada....205
Figura 82—Evaluación de la Información, Pruebas y Cumplimiento: Experiencia, Formación y Cualificaciones....205
Figura 83—Desarrollo de la Arquitectura de Seguridad de la Información: Conocimiento, Habilidades Técnicas y Habilidades de Comportamiento....205
Figura 84—Mapeo de *COBIT 5 para Seguridad de la Información* con Estándares Relacionados....208

RESUMEN EJECUTIVO

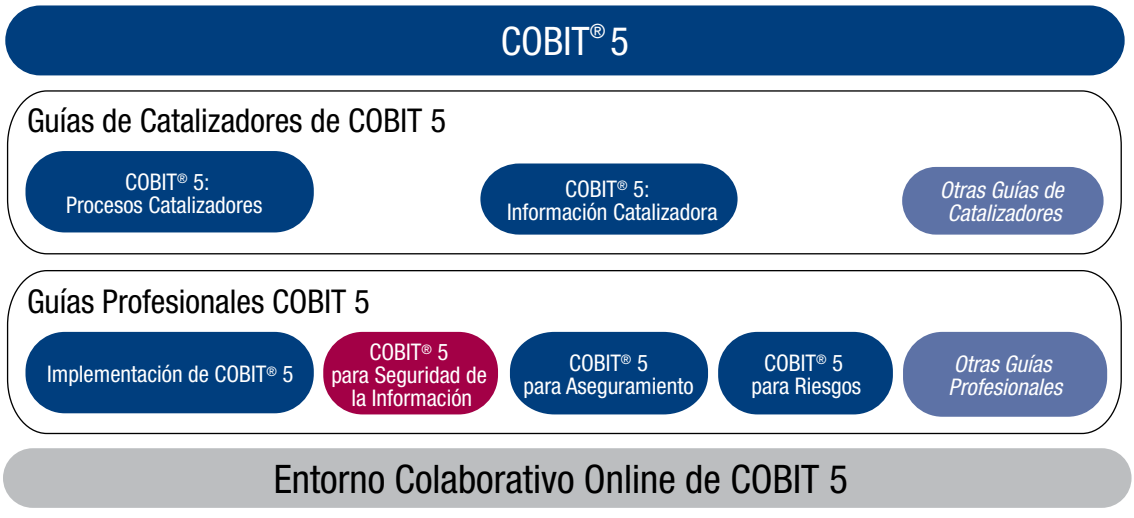
Introducción

La Información es un recurso clave para todas las empresas y desde el momento en que la información se crea hasta que es destruida, la tecnología juega un papel importante. La tecnología de la información está avanzando cada vez más y se ha generalizado en las empresas y en entornos sociales, públicos y de negocios.

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde la tecnología de la información (TI) manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 permite que las TI se gobiernen y gestionen de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y a las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de los grupos de interés internos y externos.

COBIT 5 para Seguridad de la Información, destacado en la **figura 1**, basado en el marco de COBIT 5, se enfoca en la seguridad de la información y proporciona una guía más detallada y práctica para los profesionales de seguridad de la información y otras partes interesadas a todos los niveles de la empresa (ver **figura 2**).

Figura 1—Familia de Productos COBIT 5

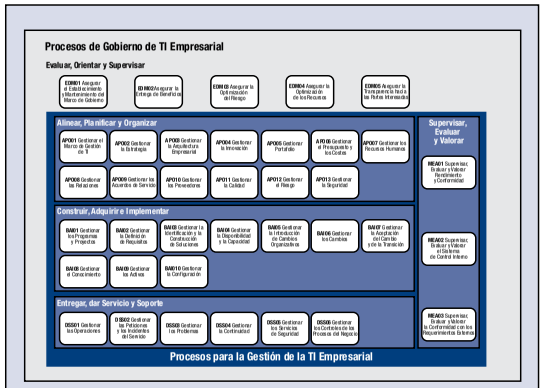


Motivos

En COBIT 5, los procesos APO13 *Gestionar la seguridad,* DSS04 *Gestionar la continuidad* y DSS05 *Gestionar los servicios de seguridad* proporcionan una guía básica acerca de cómo definir, operar y monitorizar un sistema para la gestión general de seguridad. De cualquier forma, en esta publicación se asume que la seguridad de la información se encuentra presente a lo largo de toda la empresa, con aspectos de seguridad de la información dentro de cada actividad y proceso realizado. Por lo tanto, *COBIT 5 para Seguridad de la Información* proporciona la nueva guía de ISACA para el gobierno y la gestión corporativa de la seguridad de la información.

Los motivos más importantes para el desarrollo de *COBIT 5 para Seguridad de la Información* incluyen:
- La necesidad de describir la seguridad de la información en el contexto de una empresa incluyendo:
  - Las responsabilidades funcionales de principio a fin de seguridad de la información para el negocio y TI.
  - Todos los aspectos que llevan a un gobierno y gestión efectivos de la seguridad de la información, tales como estructuras organizativas, políticas y cultura.
  - La relación y enlace de la seguridad de la información con los objetivos de la empresa.
- Una necesidad creciente de la empresa de:
  - Mantener el riesgo de información a un nivel aceptable y proteger la información contra divulgaciones no autorizadas, modificaciones involuntarias o no autorizadas y posibles intrusiones.
  - Asegurar que los servicios y sistemas se encuentran disponibles continuamente para los grupos de interés internos y externos, con el objetivo de satisfacer a los usuarios en relación al compromiso y los servicios proporcionados por TI.

Figura 2—COBIT 5 y su Relación con la Seguridad de la Información



Sección 2, Capítulo 3
Guía Detallada: Apéndice B

Estructuras Organizativas Específicas para Seguridad de la Información

- Director de Seguridad de la Información (CISO)
- Comité de Dirección de la Seguridad de la Información (ISSC)
- Gerente de Seguridad de la Información (ISM)
- Otros roles y estructuras relacionadas

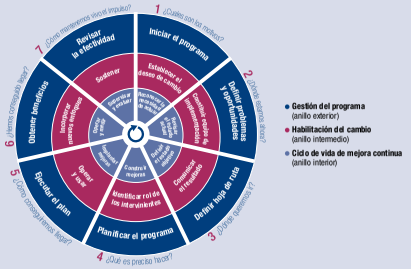
Sección II, Capítulo 4
Guía Detallada: Apéndice C

Cultura, Ética y Comportamiento Deseados Específicos para Seguridad de la Información

- La seguridad de la información se practica en las operaciones diarias.
- Las personas respetan la importancia de las políticas y principios de la seguridad de la información.
- Las personas poseen un nivel detallado y suficiente de orientación en seguridad de la información y se les anima a participar y cuestionar la situación actual de seguridad de la información.
- Todo el personal es responsable de que se proteja la información de la empresa.
- Las partes interesadas están informadas de cómo identificar y responder a las amenazas en el contexto de la empresa.
- La Dirección respalda y anticipa las innovaciones.
- La Dirección de negocio se compromete a colaborar transversalmente de manera continuada para conseguir programas de seguridad de la información efectivos y eficientes.
- La alta dirección reconoce el valor para el negocio de la seguridad de la información.

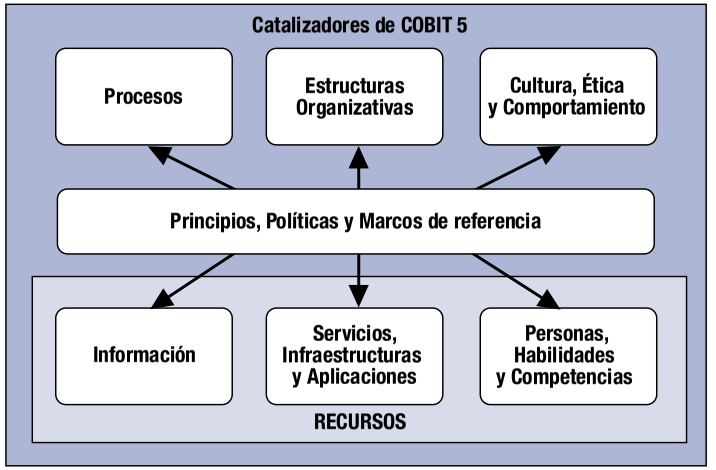
Sección 2, Capítulo 5
Guía Detallada: Apéndice D

Adaptar *COBIT 5 para seguridad de la información* a un entorno empresarial

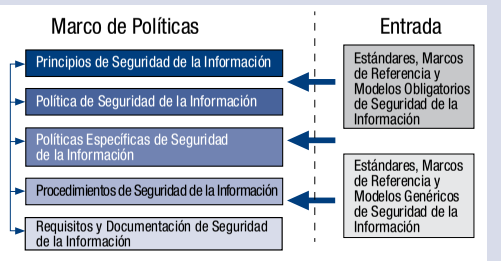


Sección III

Catalizadores de COBIT 5



Principios, Políticas y Marcos específicos para seguridad de la información



Sección II, Capítulo 2
Guía Detallada: Apéndice A

Tipos de Información Específicos para Seguridad de la Información

- Estrategia de Seguridad de la Información
- Presupuesto de Seguridad de la Información
- Plan de Seguridad de la Información
- Políticas
- Requerimientos de Seguridad de la Información
- Material de Concienciación
- Informes de Revisión de Seguridad de la Información
- Perfil de Riesgo de la Información
- Cuadro de Mando de Seguridad de la Información

Sección II, Capítulo 6
Guía Detallada: Apéndice E

Servicios, Infraestructura y Aplicaciones Específicos para Seguridad de la Información

- Proporcionar una arquitectura de seguridad.
- Proporcionar concienciación sobre seguridad.
- Proporcionar un desarrollo seguro.
- Proporcionar evaluaciones de seguridad.
- Proporcionar sistemas adecuadamente asegurados y configurados, en línea con los requerimientos y la arquitectura de seguridad.
- Proporcionar accesos a los usuarios y derechos de acceso de acuerdo con los requerimientos del negocio.
- Proporcionar una adecuada protección frente a software malicioso, ataques externos e intentos de intrusión.
- Proporcionar una adecuada respuesta a incidentes.
- Proporcionar pruebas de seguridad.
- Proporcionar servicios de monitorización y alerta par a eventos relacionados con la seguridad.

Sección II, Capítulo 7
Guía Detallada: Apéndice F

Personas, Habilidades y Competencias Específicas para Seguridad de la Información

- El gobierno de la seguridad de la información.
- La formulación de la estrategia de seguridad de la información.
- La gestión de riesgos de la información.
- El desarrollo de la arquitectura de seguridad de la información.
- Las operaciones de seguridad de la información.
- La evaluación, las pruebas y el cumplimiento de la información.

Sección II, Capítulo 8
Guía Detallada: Apéndice G

  – Cumplir con el número creciente de leyes y regulaciones relevantes, así como con requisitos contractuales y políticas internas para la seguridad y protección de la información y sistemas y proporcionar transparencia sobe el nivel de cumplimiento.
  – Alcanzar todo lo anterior a la vez que se contiene el coste de servicios de TI y la protección de la tecnología.
- La necesidad de conectarse y, cuando sea relevante, alinearse con otros marcos y estándares importantes en el mercado. El mapeo no exhaustivo (**apéndice H**) ayudará a los grupos de interés a entender la relación entre los diferentes marcos, buenas prácticas y estándares, además de cómo pueden ser usados de forma conjunta y complementarse bajo el paraguas de *COBIT 5 para Seguridad de la Información*.
- La necesidad de unir las investigaciones, marcos y guías principales de ISACA con un foco principal en el Modelo de Negocio para Seguridad de la Información (BMIS) y COBIT, y considerando también Val IT, Risk IT, el Marco de Aseguramiento TI (ITAF), la publicación titulada *Board Briefing on IT Governance* y el recurso Llevando el Gobierno hacia Adelante (TGF).

Además de estos motivos principales para el desarrollo de *COBIT 5 para Seguridad de la Información* está el hecho de que la seguridad es esencial en las operaciones diarias de las empresas. Las brechas en la seguridad de la información pueden llevar a un impacto sustancial en la empresa debido a, por ejemplo, daños financieros u operativos. Adicionalmente, la empresa puede estar expuesta a impactos externos como riesgos de reputación o legales, que pueden poner en peligro las relaciones con clientes y empleados, e incluso la supervivencia de la empresa.

Los siguientes ejemplos ilustran la necesidad de un mayor y mejor acercamiento sistemático a la seguridad de la información:
- Una infraestructura crítica nacional depende de los sistemas de información, y una intrusión exitosa podría provocar un impacto significativo en la economía y en la seguridad humana.
- Información financiera no pública que podría ser usada para obtener beneficios económicos.
- Divulgación de información confidencial que puede causar problemas a las empresas, así como daños de reputación o poner en peligro relaciones de negocio.
- Intrusión en redes comerciales, por ejemplo, para obtener datos de tarjetas de crédito o de otros medios de pago, que puede llevar a un daño de reputación y financiero sustancial debido a multas, así como un mayor escrutinio por parte de organismos reguladores.
- El espionaje industrial puede permitir que se copien secretos comerciales e incrementar la competencia entre empresas manufactureras.
- Filtraciones en la inteligencia nacional o militar que pueden resultar en un daño a las relaciones políticas.
- Una filtración de datos personales puede resultar en pérdidas financieras y en esfuerzos innecesarios para reconstruir la reputación financiera del individuo.
- Costes significativos no planificados (tanto financieros como operacionales) relacionados con contener, investigar y remediar brechas de seguridad, que pueden impactar a cualquier empresa que haya sufrido una brecha.

Beneficios

Utilizar *COBIT 5 para Seguridad de la Información* proporciona a la empresa una serie de capacidades relacionadas con la seguridad de la información que pueden resultar en beneficios como:
- Menor complejidad y mayor coste-beneficio debido a una mejorada y más fácil integración de estándares buenas prácticas y/o guías específicas del sector de seguridad de la información.
- Mayor satisfacción de usuario con la estructura y resultados de seguridad de la información.
- Mejor integración de la seguridad de la información en la empresa.
- Toma de decisiones de riesgo con conocimiento y conciencia del riesgo.
- Mejor prevención, detección y recuperación.
- Reducción (del impacto) de los incidentes de seguridad de la información.
- Soporte mejorado a la innovación y la competitividad.
- Mejor gestión de los costes relacionados con la función de seguridad de la información.
- Mayor conocimiento de la seguridad de la información.

Estos beneficios son obtenidos al hacer uso de las capacidades de *COBIT 5 para Seguridad de la Información* mostrados en la **figura 3**.

Figura 3— Capacidades *COBIT 5 para Seguridad de la Información*	
Capacidad *COBIT 5 para Seguridad de la Información*	**Descripción**
Visión actualizada de gobierno	*COBIT 5 para Seguridad de la Información* proporciona una visión más actualizada para un gobierno y gestión de seguridad de la información a través del alineamiento con COBIT 5, la Organización Internacional de Normalización (ISO)/Comisión Electrotécnica Internacional (IEC) 38500 y otras iniciativas para gobierno de TI. Durante el desarrollo de *COBIT 5 para Seguridad de la Información,* t se han analizado las guías y estándares más importantes existentes. *COBIT 5 para Seguridad de la Información se alinea con otros marcos, estándares y modelos del mercado, como la serie ISO/IEC 27000, el estándar de Buenas Prácticas para Seguridad de la Información (ISF), y con BMIS.* *Adicionalmente, se han analizado otros documentos ofrecidos para gobierno de seguridad de la información de ISACA durante el desarrollo de COBIT 5 para Seguridad de la Información,* como son el *Gobierno de Seguridad de la Información: Guía para Gestores de Seguridad de la Información* y *Gobierno de Seguridad de la Información: Guía para Comités de Dirección* y *Ejecutivos, 2ª edición.* .
Diferenciación clara entre gobierno y gestión	COBIT 5 permite aclarar los roles de gobierno y de gestión, proporcionando una diferenciación entre ellos, con un modelo de proceso que ha sido revisado y que refleja esta diferenciación, mostrando cómo se relacionan entre sí.
Visión extremo a extremo	*COBIT 5 para Seguridad de la Información* es un modelo de proceso que integra tanto responsabilidades funcionales del negocio como de TI. Proporciona una clara distinción entre el gobierno de la seguridad de la información y las prácticas de gestión de la seguridad de la información, marcando responsabilidades en los diferentes niveles de la empresa, que abarcan todos los pasos del proceso de principio a fin.
Guía holística	El marco de *COBIT 5 para Seguridad de la Información* proporciona una guía completa y holística para la seguridad de la información. Holística significa que se presta atención a todos los procesos y catalizadores, incluyendo información, estructuras, cultura y políticas, así como su interdependencia.

COBIT 5 para Seguridad de la Información está basado en el marco de COBIT 5, del que se ha filtrado y complementado la información relevante a seguridad con guías más detalladas y específicas, asegurando una consistencia con la arquitectura del producto de COBIT 5. COBIT 5 comienza con las expectativas e inquietudes de los grupos de interés relacionados con las TI de la empresa. Todas las guías pueden ser relacionadas con asuntos de los grupos de interés y, por lo tanto, la seguridad de la información ayuda a soportar la misión del negocio y a alcanzar sus metas.

Público Objetivo

COBIT 5 para Seguridad de la Información está orientado para todos los grupos de interés de seguridad de la información. La audiencia más obvia son los Directores de Seguridad de la Información (CISO), Gerentes de Seguridad de la Información (ISM) y otros profesionales de seguridad de la información. No obstante, la seguridad de la información es responsabilidad de todos los grupos de interés dentro de la empresa, incluyendo a todos los empleados y otros grupos de interés, incluyendo terceras partes. Por lo tanto, ésta publicación puede ser de interés para todas las partes de la empresa.

Convenciones Utilizadas y Resumen

COBIT 5para Seguridad de la Información se refiere a varios catalizadores como roles, puestos, comités, procesos y políticas. Las características únicas de cada empresa pueden ocasionar que estos catalizadores sean utilizados de muchas formas distintas para proporcionar seguridad de la información de una forma óptima. *COBIT 5 para Seguridad de la Información* utiliza guías y ejemplos que proporcionan una visión completa que explica cada concepto de COBIT 5 desde una perspectiva de seguridad de la información.

Para guiar al lector a través de la extensa colección de información, *COBIT 5 para Seguridad de la Información* festá formado por tres secciones y ocho apéndices.

Cada sección contiene varios capítulos. Dentro de cada capítulo, en caso de ser necesario, se han utilizado algunas marcas que permiten guiar al lector a través de la explicación. Adicionalmente, se han utilizado cajas de color azul y gris para lo siguiente:
- La caja azul se utiliza para marcar los puntos de atención relevantes a seguridad de la información.
- La caja gris refleja material que se utiliza para enlazar la información con algún otro tema relevante. Las secciones también hacen referencia a los apéndices para obtener mayor información.

A continuación se describe cada sección y su interrelación con otras:
- **Sección I**—Profundiza en el tema de **seguridad de la información** y describe brevemente cómo la arquitectura de COBIT 5 puede ser adaptada a necesidades específicas de seguridad de la información. Esta sección proporciona una base conceptual que es utilizada en el resto de la publicación.
- **Sección II**—Profundiza en el **uso de los catalizadores de COBIT 5 para implementar seguridad de la información.** El gobierno de las TI corporativas es sistemático y se apoya en un conjunto de catalizadores. En esta sección se introduce el concepto de catalizadores específicos para seguridad, los cuales se explican utilizando ejemplos prácticos. En los apéndices se proporciona una guía detallada sobre estos catalizadores.
- **Sección III**—Profundiza en cómo **adaptar COBIT 5 para seguridad de la información a un entorno empresarial.** Esta sección contiene guías de cómo se pueden implementar las iniciativas de seguridad de la información y proporciona un mapeo con otros estándares y marcos dentro del área de seguridad de la información y *COBIT 5 para Seguridad de la Información.*

Los **apéndices** contienen guías detalladas basadas en los catalizadores introducidos en la sección II:
- **Apéndice A**—Guía detallada acerca de los principios, políticas y marcos catalizadores
- **Apéndice B**—Guía detallada acerca de los procesos catalizadores
- **Apéndice C**—Guía detallada acerca de las estructuras organizativas catalizadoras
- **Apéndice D**—Guía detallada acerca la cultura, ética y comportamientos catalizadores
- **Apéndice E**—Guía detallada acerca de la información catalizadora
- **Apéndice F**—Guía detallada acerca de los servicios, infraestructura, y aplicaciones catalizadoras
- **Apéndice G**—Guía detallada acerca de las personas, habilidades y competencias catalizadoras
- **Apéndice H**—Mapeos detallados de *COBIT 5 para Seguridad de la Información* con otros estándares de seguridad de la información

Las secciones de **Acrónimos** y **Glosario** spermiten clarificar las abreviaciones y términos utilizados únicamente en esta publicación. Para términos normalizados, por favor referirse al Glosario de Términos de ISACA que se puede encontrar en *www.isaca.org/Glossary*.

Página dejada en blanco intencionadamente

Sección I. Seguridad de la Información

Capítulo 1
Definición de Seguridad de la Información

ISACA define a la seguridad de la información como algo que:

> *Asegura que dentro de la empresa, la información está protegida contra su divulgación a usuarios no autorizados (confidencialidad), modificación inadecuada (integridad) y su falta de acceso cuando se la necesita (disponibilidad).*

- La confidencialidad significa preservar las restricciones autorizadas sobre el acceso o divulgación, incluyendo los medios para proteger la privacidad y la información propietaria.
- La Integridad significa proteger contra la destrucción o modificación inadecuada de la información e incluye asegurar el no repudio y autenticidad de la información.
- La disponibilidad significa asegurar que se puede acceder y usar la información de manera confiable y en el momento adecuado.

Aunque existen muchas otras definiciones del término, esta definición proporciona los fundamentos de seguridad de la información ya que cubre los conceptos de confidencialidad, integridad y disponibilidad (CIA). Es importante destacar que mientras el concepto CIA es globalmente aceptado, hay otros usos más amplios del término “integridad” en un contexto más amplio del negocio. COBIT 5 cubre este término dentro del catalizador información como objetivos de completitud y precisión de la información. *COBIT 5 para Seguridad de la Información* se limita a la perspectiva de seguridad de este término y se apoya en esta definición para describir cómo la seguridad de la información puede aplicarse en la vida real, considerando los principios de COBIT 5.

La seguridad de la información es un catalizador de negocio que está intrínsecamente unido a la confianza de las partes interesadas, ya sea tratando los riesgos de negocio o creando valor para la empresa como una ventaja competitiva. En un momento en que la importancia de la información y las tecnologías relacionadas con ella están creciendo en cada aspecto del mundo de los negocios y la vida pública, la necesidad de mitigar el riesgo sobre la información, lo que incluye proteger la información y los activos de TI relacionados con ella de amenazas que cambian continuamente, se está intensificando constantemente. El incremento en la regulación en el entorno de negocios se suma a la concienciación de los Consejos de Administración sobre la criticidad de la seguridad de la información para la información y los activos de TI relacionados.

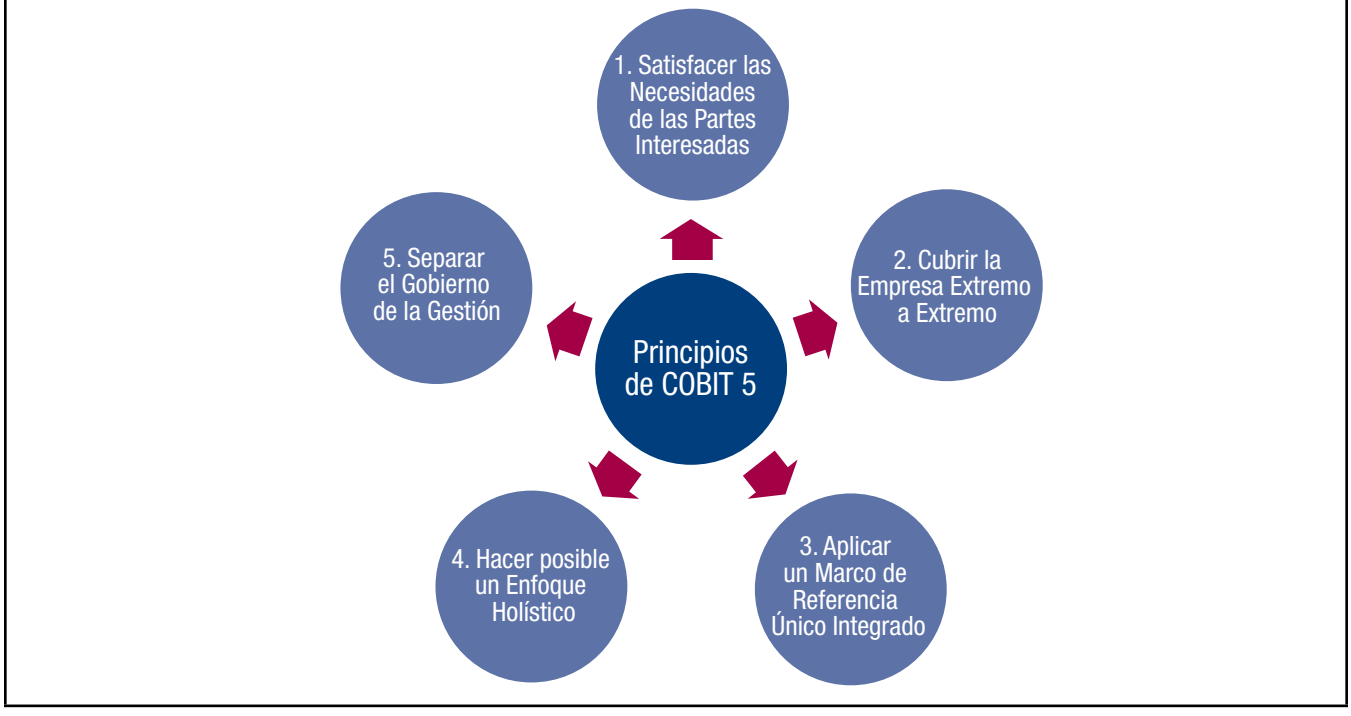
Página dejada en blanco intencionadamente

Capítulo 2
Principios de COBIT 5

2.1 Visión General

COBIT 5 para Seguridad de la Información se basa en los mismos principios que el marco de COBIT 5 (**figura 4**).

Figura 4—Principios de COBIT 5



El texto que sigue describe brevemente cada principio y su relevancia para la seguridad de la información.

2.2 Principio 1. Satisfacer las Necesidades de las Partes Interesadas

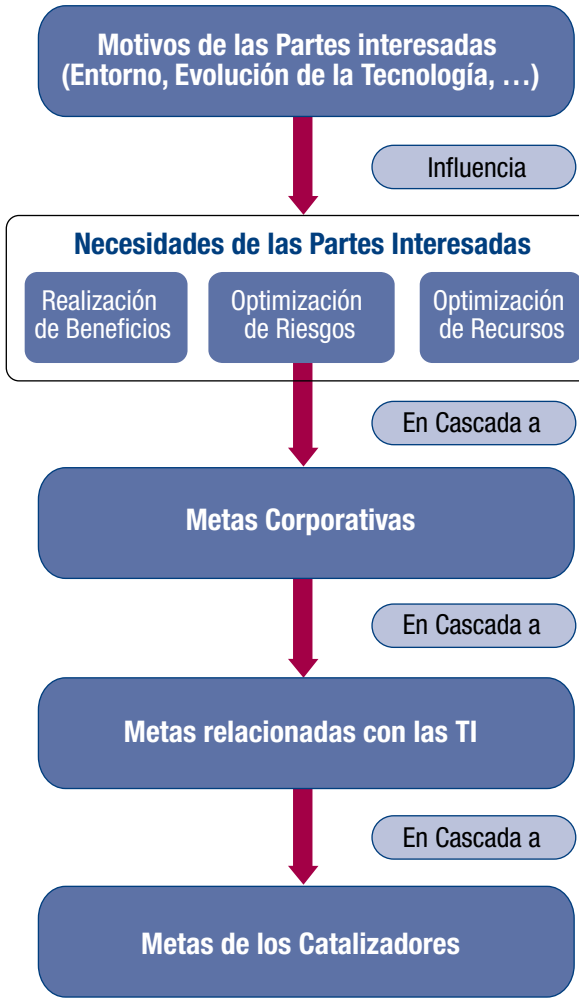
Las empresas existen para crear valor a sus partes interesadas —incluyendo las partes interesadas en la seguridad de la información— al mantener un equilibrio entre la consecución de beneficios, la optimización del riesgo y del uso de recursos. La optimización del riesgo es lo que se considera más importante para la seguridad de la información.

Cómo cada empresa tiene objetivos diferentes, debe utilizar la cascada de metas para personalizar COBIT 5 a su propio contexto. En la cascada de metas, ilustrada en la **figura 5**, las necesidades de las partes interesadas, que están influenciadas por diferentes motivos, se traducen y concretan en metas operativas de empresa que deben satisfacerse. Para cumplir con estas metas empresariales, se requiere a su vez alcanzar las metas relacionadas con TI, y finalmente traducirse en metas para los diferentes catalizadores.

La seguridad de la información es una necesidad importante para las partes interesadas, y esto se traduce en metas relacionadas con seguridad de la información para la empresa, para TI y finalmente para los catalizadores que los soportan.

En *COBIT 5 para Seguridad de la Información*,se definen metas específicas de seguridad de la información para procesos como apoyo a las necesidades de las partes interesadas relacionadas con la seguridad de la información. De la misma manera, se definen metas específicas para el resto de catalizadores relacionados con la seguridad de la información (sección II).

Figura 5—Visión General de la Cascada de Metas de COBIT 5



2.3 Principio 2. Cubrir la Empresa Extremo-a-Extremo

COBIT 5 integra el gobierno de las TI corporativas con en el gobierno de la empresa al:
- Cubrir todas las funciones y procesos que forman parte de la empresa. COBIT 5 no se centra sólo en "la función de TI", sino que trata la información y las tecnologías relacionadas con ella como activos que deben ser tratados de la misma forma que se hace con cualquier otro activo de la empresa.
- Considerar que todos los catalizadores relacionados con el gobierno y gestión de las TI abarcan toda la empresa de extremo a extremo, es decir, incluyendo a todo y a todos, internos y externos, que sean relevantes para el gobierno y gestión de la información de la empresa y las TI relacionadas con ella. Aplicando este principio a la seguridad de la información, *COBIT 5 para Seguridad de la Información* cubre a todas las partes interesadas, funciones y procesos que forman parte de la empresa y son relevantes para la seguridad de la información.

2.4 Principio 3. Aplicar un Marco de Referencia Único Integrado

Existen muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades relacionadas con las TI. COBIT 5 es completo en cuanto a la cobertura de la empresa, y proporciona una base para integrar de manera efectiva otros marcos de referencia, estándares y prácticas que se utilicen. Como único marco de referencia integrado, sirve como una fuente consistente e integrada de guía en un lenguaje común no técnico y agnóstico en cuanto a la tecnología. COBIT 5 se alinea con otros estándares y marcos de referencia relevantes, y de esta manera permite a la empresa utilizarlo como el marco de referencia general para el gobierno y gestión de las TI de la empresa.

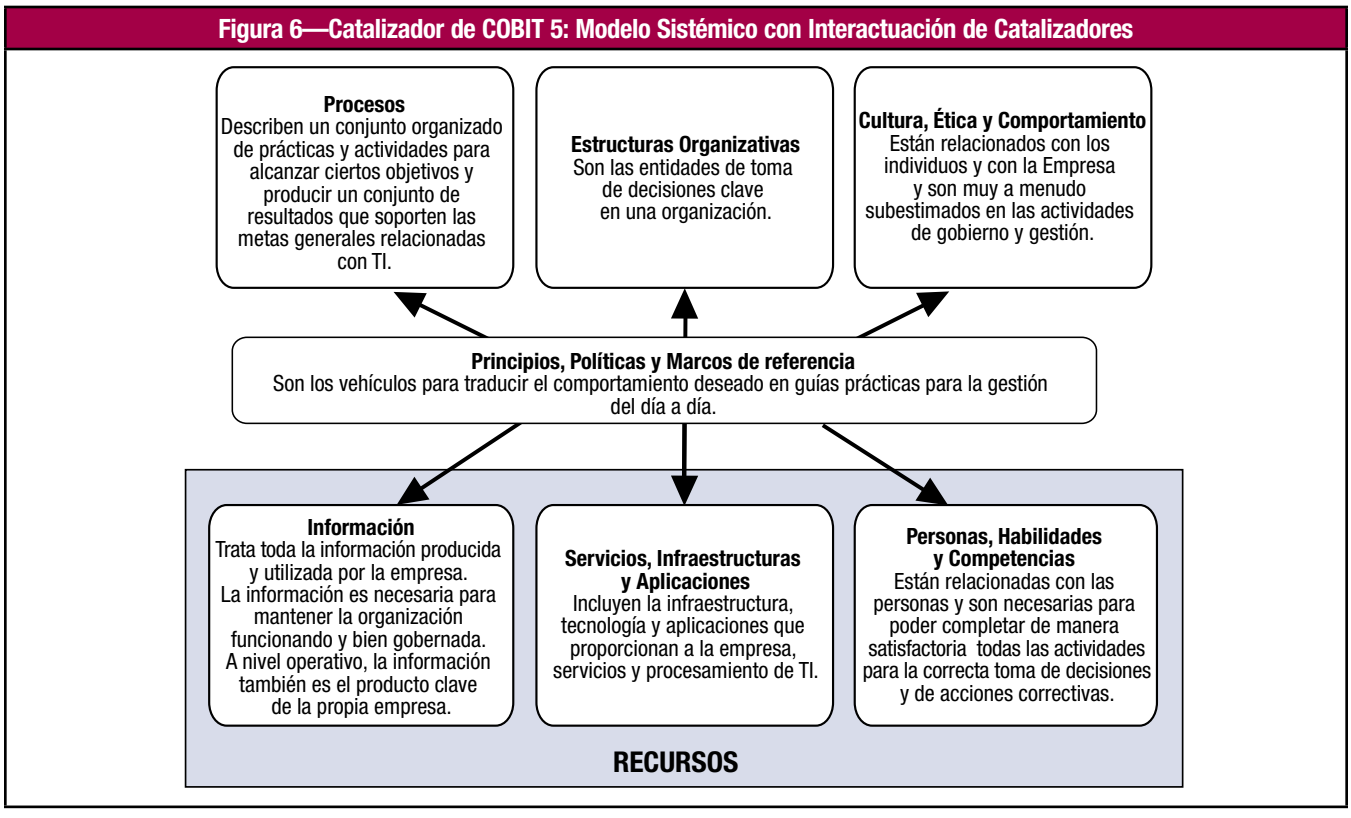
Más específicamente, *COBIT 5 para Seguridad de la Información* reúne conocimientos previamente distribuidos entre los diferentes marcos y modelos de ISACA (COBIT, BMIS, Risk IT, Val IT) con guías de otros importantes estándares relacionados con la seguridad de la información tales como la serie ISO/IEC 27000, el Estándar de Buenas Prácticas para Seguridad de la Información de ISF y el SP800-53A del U.S. National Institute of Standards and Technology (NIST).

2.5 Principio 4. Hacer Posible un Enfoque Holístico

Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes que interactúan. COBIT 5 define un conjunto de catalizadores (*enablers*) para apoyar la implementación de un sistema de gobierno y gestión global para las TI y la información de la empresa. Los catalizadores son factores que, individual y colectivamente, influyen en que algo funcione – en este caso, el gobierno y la gestión de las TI de la empresa y, relacionado con eso, el gobierno de la seguridad de la información. Los catalizadores se dirigen por la cascada de metas, es decir, las metas de alto nivel de las TI definen lo que los diferentes catalizadores deberían lograr.

El marco de COBIT 5 define siete categorías de catalizadores (**figura 6**).

Figura 6—Catalizador de COBIT 5: Modelo Sistémico con Interactuación de Catalizadores



En la sección II, se tratan y analizan todos los catalizadores interconectados requeridos para una adecuada seguridad de la información, presentando una estrategia holística y sistémica hacia la seguridad de la información.

2.6 Principio 5. Separar el Gobierno de la Gestión

El marco de COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. La visión de COBIT 5 en esta fundamental distinción entre gobierno y gestión es:

Gobierno

El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

En la mayoría de las empresas, el gobierno es responsabilidad del consejo de administración bajo la dirección de su presidente.

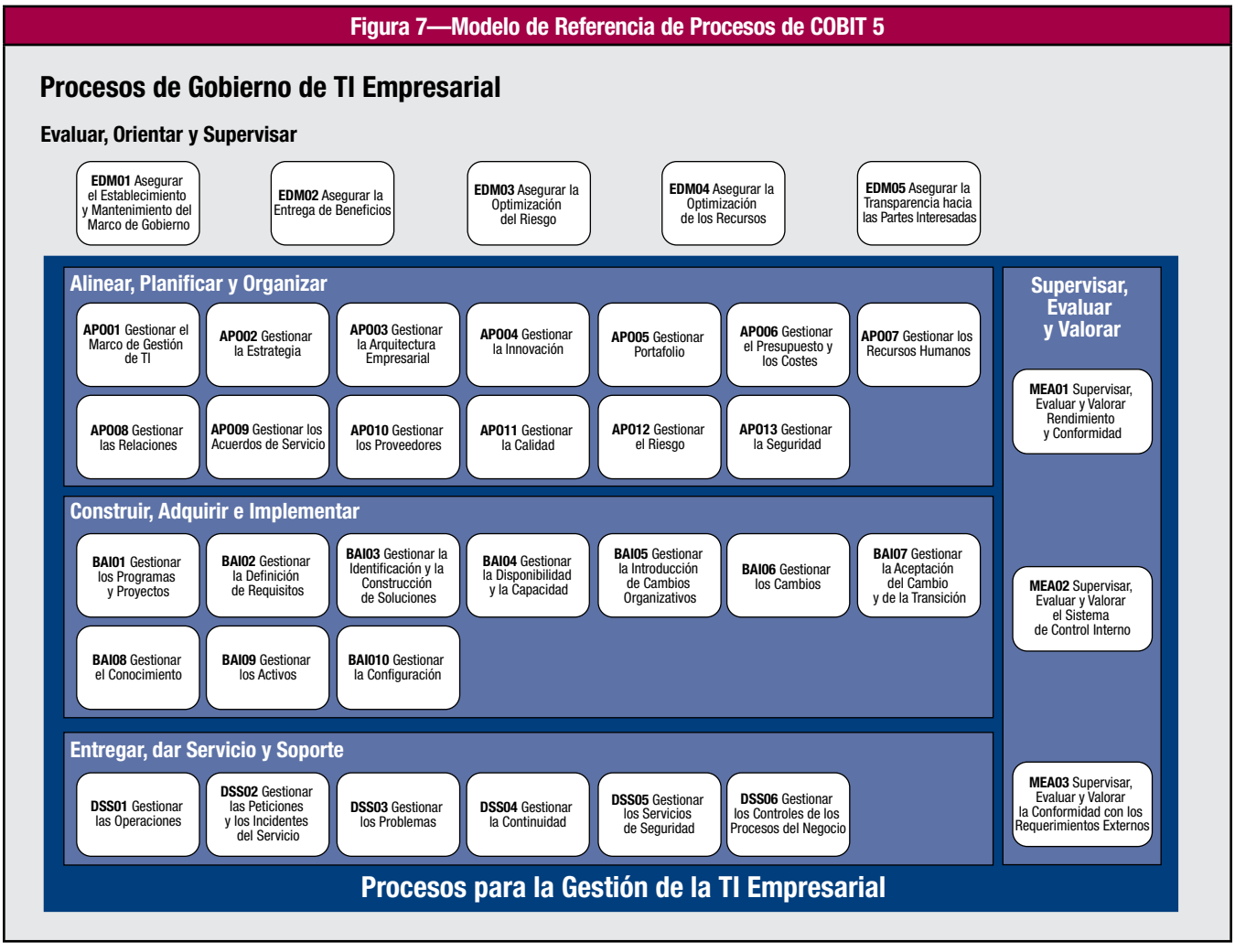
Gestión

La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

En la mayoría de las empresas, la gestión es responsabilidad de la dirección ejecutiva bajo la dirección del Director General Ejecutivo (CEO).

En la práctica, los diferentes roles del gobierno y gestión de la seguridad de la información se hacen visibles mediante el modelo de procesos de COBIT 5, que incluye procesos de gestión y procesos gobierno, cada grupo con sus propias responsabilidades. Esto se representa en la **figura 7** y está explicado detalladamente en la sección II.

Figura 7—Modelo de Referencia de Procesos de COBIT 5



Sección II. Uso de los Catalizadores de COBIT 5 para Implantar la Seguridad de la Información en la Práctica

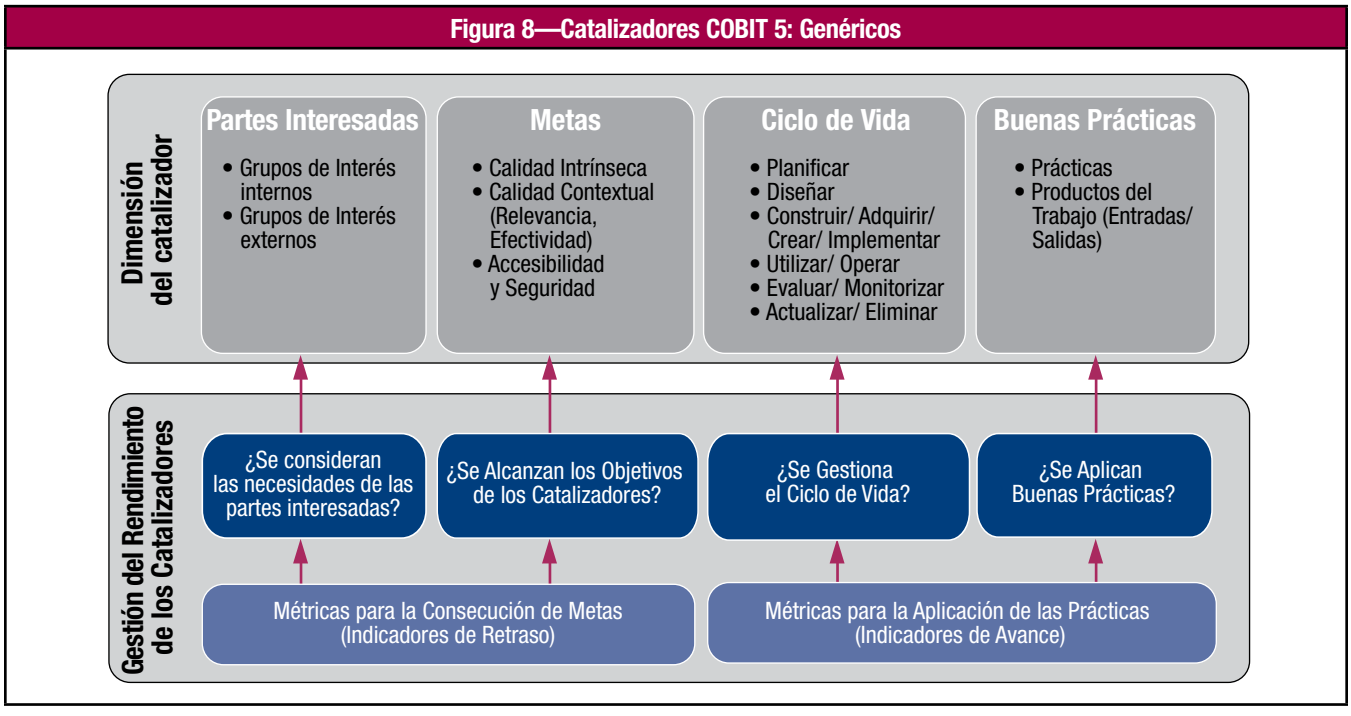
Capítulo 1
Introducción

Esta sección describe cómo los catalizadores de COBIT 5, tal como se introdujo en la sección I, pueden aplicarse en situaciones prácticas y cómo estos catalizadores pueden usarse para implantar un efectivo y eficiente gobierno y gestión de la seguridad de la información en la empresa.

1.1 El Modelo Genérico de Catalizadores

Los catalizadores definidos en COBIT 5 tienen un conjunto de dimensiones comunes (**figura 8**). Este conjunto:
- Proporciona una manera simple y estructurada de tratar con los catalizadores
- Permite a una entidad manejar sus complejas interacciones
- Facilita resultados exitosos de los catalizadores

Figura 8—Catalizadores COBIT 5: Genéricos



Las cuatro dimensiones comunes de los catalizadores son:
- **Grupos de interés**—Cada catalizador tiene grupos de interés (partes que juegan un rol activo y/o tienen un interés en el catalizador). Por ejemplo, los procesos tienen diferentes partes que realizan actividades y/o tienen un interés en los resultados del proceso; las estructuras organizativas tienen grupos de interés, que son parte de las estructuras, cada uno con sus propios roles e intereses, que son parte de las estructuras. Los grupos de interés pueden ser internos o externos a la empresa, cada uno de ellos con sus propias necesidades e intereses, algunas veces contrarios entre sí. Las necesidades de los grupos de interés se traducen en metas corporativas, que a su vez se traducen en objetivos de TI para la empresa..
- **Metas**—Cada catalizador tiene varias metas (resultados esperados) y los catalizadores proporcionan valor por la consecución de dichas metas. Las metas del catalizador son el paso final en la cascada de metas de COBIT 5.

  Las metas pueden ser divididas a su vez en diferentes categorías:
  – **Calidad intrínseca**—Medida en que los catalizadores proporcionan resultados precisos, objetivos y de confianza.
  – **Calidad contextual**—Medida en que los catalizadores y sus resultados son aptos para el propósito dado el contexto en el que operan. Por ejemplo, los resultados deben ser relevantes, completos, actuales, apropiados, consistentes, comprensibles y fáciles de usar.

  - **Accesibilidad y seguridad**—Medida en la que los catalizadores son accesibles (disponibles cuando y si se necesitan) y seguros (el accesos está restringido a aquellos autorizados y que lo necesitan).
- **Ciclo de vida**—Cada catalizador tiene un ciclo de vida, desde el comienzo pasando por su vida útil / operativa hasta su eliminación. Las fases del ciclo de vida consisten en:
  - Planificar (incluye el desarrollo y selección de conceptos)
  - Diseñar
  - Construir / adquirir / crear / implementar
  - Utilizar / operar
  - Evaluar / monitorizar
  - Actualizar / eliminar
- **Buenas Prácticas**—Para cada uno de los catalizadores, se pueden definir buenas prácticas. Las buenas prácticas soportan la consecución de los objetivos del catalizador y proporcionan ejemplos y sugerencias sobre cómo implementar de la mejor manera el catalizador y qué productos o entradas y salidas son necesarias. Una vez que estas buenas prácticas están bien afinadas y se integran con éxito dentro de la empresa, pueden llegar a ser, mediante el seguimiento de la evolución de las necesidades de negocio y la supervisión adecuada, buenas prácticas para la empresa.

1.2 Gestión del Rendimiento de los Catalizadores

Las empresas esperan resultados positivos de la aplicación y uso de los catalizadores. Para gestionar el rendimiento de los catalizadores, las siguientes cuestiones deberán ser supervisadas y respondidas —basadas en las métricas— de manera periódica:
- ¿Se consideran las necesidades de las partes interesadas?
- ¿Se alcanzan los objetivos de los catalizadores?
- ¿Se gestiona el ciclo de vida?
- ¿Se aplican las buenas prácticas?

Los primeros dos puntos tratan con el resultado actual del catalizador. Las métricas utilizadas para medir el punto hasta el que las metas son alcanzadas pueden ser denominadas ‘indicadores de retraso’.

Los dos últimos puntos tratan con el funcionamiento actual del catalizador en sí mismo y las métricas para ellos pueden ser denominadas ‘indicadores de avance’.

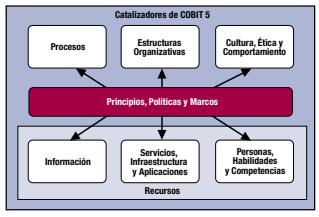
1.3 *COBIT 5 para Seguridad de la Información* y los Catalizadores

COBIT 5 para Seguridad de la información proporciona orientación específica en relación a con todos los catalizadores:
1. Las **políticas, principios y marcos de referencia** de seguridad de la información.
2. Los **procesos,** incluyendo detalles y actividades específicos de seguridad de la información.
3. Las **estructuras organizativas** específicas de seguridad de la información.
4. En términos de **cultura, ética y comportamiento,** los factores determinantes para el éxito del gobierno y la gestión de la seguridad de la información.
5. Los tipos de **información** específicos de la seguridad de la información para permitir el gobierno y la gestión de la seguridad de la información en la empresa.
6. Las **capacidades de servicio** necesarias para proporcionar seguridad de la información y las funciones relacionadas con la empresa.
7. Las **personas, habilidades y competencias** específicas para seguridad de la información.

Para cada catalizador considerado en este capítulo, se analizarán todos los componentes cuando sean relevantes o cuando la descripción genérica necesite ser concretada. Los capítulos de esta sección siguen el mismo orden que el enumerado más arriba.

Además de una descripción específica de seguridad de la información de los componentes de los catalizadores, se pueden encontrar directrices detalladas sobre estos catalizadores en los apéndices A-G.

Capítulo 2
Catalizador: Principios, Políticas y Marcos de Referencia

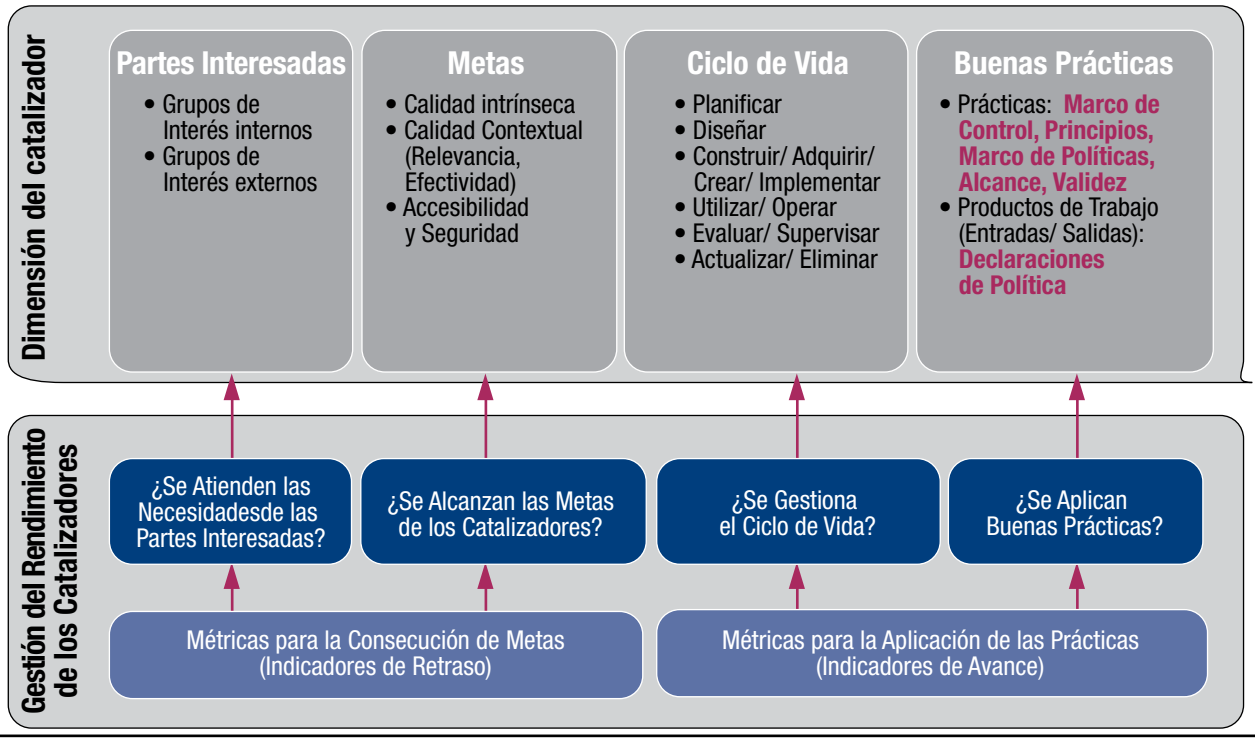


Los principios, las políticas y los marcos de referencia se refieren a los mecanismos de comunicación disponibles para trasmitir la dirección e instrucciones de los cuerpos de gobierno y de gestión. Este capítulo incluye los siguientes elementos:
1. Modelo de principios, políticas y marco de referencia
2. Principios de seguridad de la información
3. Políticas de seguridad de la información
4. Adaptar las políticas al entorno de la empresa
5. Ciclo de vida de las políticas

2.1 Modelo de Principios, Políticas y Marco de Referencia

Los principios, políticas y marcos de referencia son los medios para traducir el comportamiento deseado de los miembros del personal de la empresa con respecto a la seguridad de la información en guías formales, y sin embargo prácticas, para la gestión del día a día. Estos principios, políticas y marcos de referencia pueden estructurarse según las dimensiones que se ilustran en el modelo de catalizadores de la **figura 9**.

Figura 9—Catalizador de COBIT 5: Principios, Políticas y Marcos de Referencia



La **figura 9** muestra las diferentes componentes de los principios, políticas y marcos de referencia a alto nivel como están definidos en esta publicación. Este modelo de proceso es una extensión del modelo genérico de catalizador explicado en la **figura 8.**

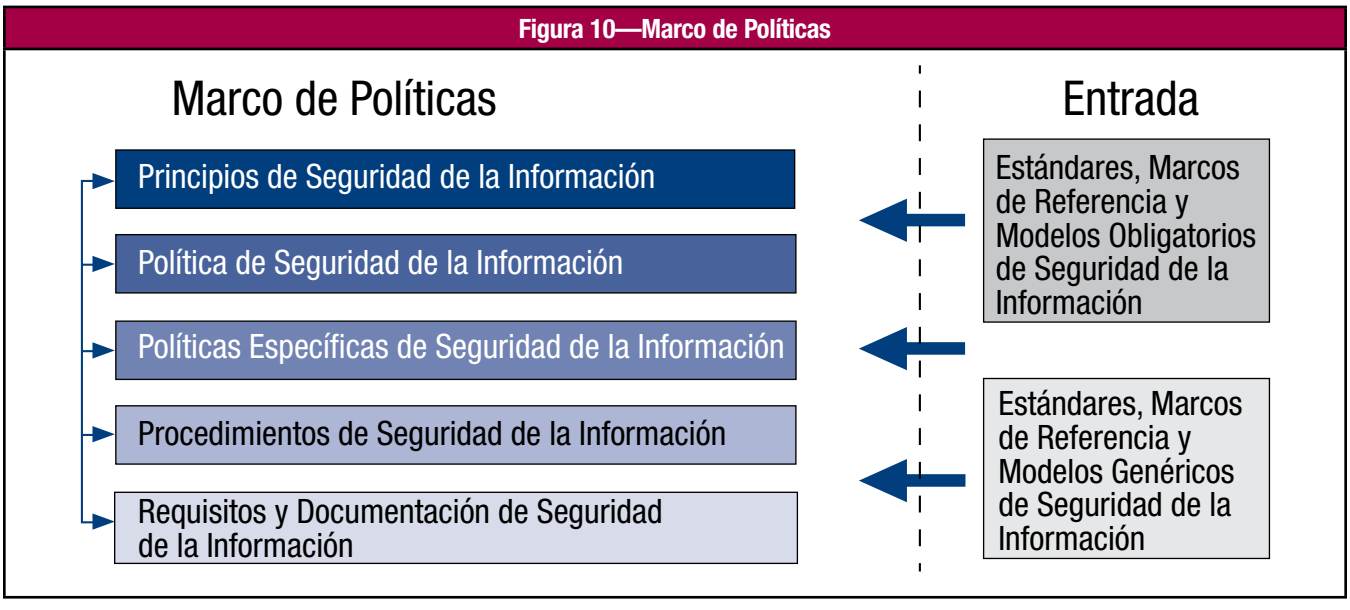
El modelo de principios, políticas y marcos de referencia indica que:
- En el caso de principios, políticas y marcos de referencia, las **partes interesadas** incluyen el Consejo y el comité ejecutivo de dirección, directores de cumplimiento, gerentes de riesgos, auditores internos y externos, proveedores de servicio, clientes y agencias reguladoras. Sus intereses están divididos: algunas partes interesadas definen y establecen las políticas mientras que las otras tienen que alinearse y cumplir con ellas.
- Los principios, políticas y marcos de referencia son los instrumentos para comunicar las reglas de la empresa en apoyo a **las metas de gobierno y los valores de la empresa,** conforme los define el Consejo y el comité ejecutivo de dirección. Los principios deberían estar limitados en número y expresados en un lenguaje sencillo. Las políticas proporcionan una directriz más detallada respecto a cómo llevar a la práctica los principios; influyen respecto a cómo la toma de decisiones se alinea con dichos principios.

- Las políticas tienen un **ciclo de vida** que debe apoyar la consecución de las metas definidas. Los marcos de referencia son clave porque proporcionan la estructura para definir una directriz coherente, por ejemplo, un marco de referencia para políticas proporciona la estructura con la que se pueden crear y mantener un conjunto coherente de éstas y proporciona también el ámbito en el que movernos y navegar dentro de y entre ellas.
- Las **buenas prácticas** requieren que las políticas formen parte de un marco de políticas general, proporcionando una estructura (jerárquica) a la que deberían ceñirse todas las políticas y actuando de enlace con los principios subyacentes.

El marco de políticas necesita definir:
- Las personas que aprueban las políticas de la empresa
- Las consecuencias de no cumplir con la política
- Los mecanismos para la gestión de las excepciones
- La forma en la que se comprobará y medirá el cumplimiento con la política

La responsabilidad de que se realice el desarrollo y mantenimiento del marco de referencia y las políticas relacionadas se atribuye al presidente del comité de supervisión de (Information Security Steering Committee, ISSC). El marco de referencia se puede usar como referente al que ajustar todas las políticas/procedimientos y vincularlas con los principios identificados. En la práctica, el marco de referencia informa a los profesionales de la seguridad de la información y a otros usuarios de las políticas de seguridad de la información sobre cómo consultar las guías disponibles, como se representa en la **figura 10**.

Figura 10—Marco de Políticas



Los requisitos y documentación de seguridad de la información detallados deben consultarse en primer lugar cuando aparece un problema operativo. En caso de que la guía operativa y/o técnica apropiada no exista, el usuario puede consultar los procedimientos de seguridad de la información y a continuación **las políticas relacionadas con la seguridad de la información.** Estas políticas cubren un área complementaria de seguridad de la información y proporcionan una guía táctica. La política de seguridad de la información consiste en directrices de alto nivel de seguridad de la información. Un usuario puede consultar esta **política general** cuando no existe una política detallada. Finalmente, el usuario necesita aplicar los **principios generales** cuando la política general de seguridad de la información no sea clara sobre el asunto.

Cuando un usuario ha identificado la necesidad de una guía más detallada, se debería comunicar siempre al gestor de la seguridad de la información.

Para el desarrollo de guías específicas para la empresa, el ISSC (o la función delegada) puede usar los estándares de seguridad de la información. En este contexto, el uso de estándares, marcos de referencia y modelos genéricos y obligatorios como entrada para el marco de políticas puede diferenciarse. Dependiendo de la situación, es necesario tener en cuenta estándares, marcos de referencia y modelos obligatorios cuando se desarrollan los principios, políticas, procedimientos y requerimientos. Por ejemplo, cuando las empresas toman la decisión de negocio de certificarse en ISO/IEC 27001, dichas organizaciones necesitan cumplir con el estándar ISO/IEC 27001. Las empresas que proporcionan y aceptan tarjetas de crédito necesitan cumplir con los Estándares de Seguridad de Datos para la Industria de Pagos con Tarjeta (PCI DSS). En estos casos, los estándares relacionados que se usan serán de carácter obligatorio debido a las decisiones de negocio. Como alternativa, el ISSC puede querer usar estándares o guías de seguridad de la información como buenas prácticas genéricas para desarrollar eficientemente los principios, políticas, procedimientos y requisitos requeridos.

2.2 Principios de Seguridad de la Información

Los principios de seguridad de la información comunican las reglas de la empresa para dar soporte a los objetivos de gobierno y los valores empresariales, según haya sido definidos por el Consejo de Administración y la Dirección Ejecutiva. Estos principios necesitan:
- Ser limitados en número
- Estar expresados en un lenguaje simple y enunciar, tan claro como sea posible, los valores fundamentales de la empresa.

En 2010, tres organizaciones globales líderes en seguridad de la información – ISACA, ISF e International Information System Security Certification Consortium [(ISC)²] – unieron fuerzas para desarrollar 12 principios independientes y no propietarios que ayudarán a los profesionales de seguridad de la información a añadir valor a sus organizaciones mediante un apoyo al negocio con éxito y la promoción de las buenas prácticas de seguridad de la información. Estos principios están estructurados para dar soporte a tres tareas:

1. Dar soporte al negocio:
   - **Centrarse en el negocio** para asegurar que la seguridad de la información está integrada en las actividades de negocio esenciales.
   - **Dar calidad y valor a las partes interesadas** para asegurar que la seguridad de la información aporta valor y cumple con los requisitos de negocio.
   - **Cumplir con los requisitos legales y regulatorios relevantes** para asegurar que se cumplen las obligaciones estatutarias, se gestionan las expectativas de las partes interesadas y se evitan las penalizaciones civiles o criminales.
   - **Proporcionar información oportuna y exacta sobre el desempeño de la seguridad de la información** para dar soporte a los requisitos del negocio y gestionar el riesgo de la información.
   - **Evaluar las amenazas actuales y futuras** para analizar y evaluar las amenazas de seguridad emergentes de manera que se puedan tomar acciones oportunas e informadas para mitigar el riesgo.
   - **Promover la mejora continua en la seguridad de la información** para reducir costes, mejorar la eficiencia y eficacia y promover una cultura de mejora continua de la seguridad de la información.
2. Defender el negocio:
   - **Adoptar una estrategia basada en el riesgo** para asegurar que el riesgo se trata de forma consistente y efectiva.
   - **Proteger la información clasificada** para prevenir su revelación a personas no autorizadas.
   - Concentrarse en las aplicaciones críticas para el negocio para priorizar los escasos recursos de seguridad de la información mediante la protección de las aplicaciones de negocio en las que un incidente de seguridad tendría un mayor impacto en el negocio.
   - **Desarrollar los sistemas de forma segura** para construir sistemas de calidad y rentables en los que las personas del negocio puedan confiar.
3. Promover un comportamiento responsable en seguridad de la información:
   - **Actuar de manera profesional y ética** para asegurar que las actividades relacionadas con la seguridad de la información se desarrollan de manera fiable, responsable y efectiva.
   - **Fomentar una cultura positiva de seguridad de la información** para proporcionar una influencia de seguridad positiva en el comportamiento de los usuarios finales, reducir la probabilidad de que ocurran incidentes de seguridad y limitar su impacto potencial en el negocio.

Estos principios son genéricos y aplicables a todas las empresas. En el desarrollo de los principios de seguridad de la información exclusivos de la empresa, esta lista se puede usar como inspiración.

En el **apéndice A** se proporcionan el objetivo y la descripción para cada uno de estos principios.

2.3 Políticas de Seguridad de la Información

Las políticas proporcionan una guía más detallada de cómo poner en práctica los principios y cómo éstos influirán en la toma de decisiones. No todas las políticas relevantes están escritas y son propiedad de la función de seguridad de la información. En esta publicación se describen varias políticas y se especifica quién dirige cada política dentro de la empresa. Las políticas se estructuran en tres grupos:
- La política de seguridad de la información escrita por la función de seguridad de la información, pero dirigida por la Dirección Ejecutiva
- Las políticas específicas de seguridad de la información dirigidas por la función de seguridad de la información
- Otras políticas que puedan relacionarse con la seguridad de la información, pero que están dirigidas por otras funciones de la empresa. En estas políticas, la seguridad de la información debería influir en el desarrollo para asegurar el logro de los requisitos de seguridad de la información.

La siguiente lista de políticas relevantes es ilustrativa y no exhaustiva:
- Política de seguridad de la información
- Política de control de acceso
- Política de seguridad de la información del personal
- Política de seguridad física y ambiental
- Política de gestión de incidentes
- Política de continuidad de negocio y recuperación ante desastres
- Política de gestión de activos
- Reglas de comportamiento (uso aceptable)
- Política de adquisición, desarrollo de software y mantenimiento de sistemas de información
- Política de gestión de proveedores
- Política de gestión de comunicaciones y operaciones
- Política de cumplimiento
- Política de gestión de riesgos

Para cada una de estas políticas, en el **apéndice A** se describen los siguientes atributos:
- **Alcance**
- **Validez** (excepto para las políticas de seguridad de la información dirigidas por otras funciones dentro de la empresa)
  - **Aplicabilidad**—¿A qué áreas de la empresa se aplica esta política?
  - **Actualización y revalidación**—¿Quién es el responsable de mantener la política y cuál es la frecuencia de revalidación?
  - **Distribución**—¿Cómo se deberían distribuir las políticas en la empresa?
- **Metas** (excepto para las políticas de seguridad de la información dirigidas por otras funciones dentro de la empresa)

2.4 Adaptar las Políticas al Entorno de la Empresa

Estas políticas, y por consiguiente el marco de políticas, deberían estar alineadas con los principios y los objetivos, la estrategia y el apetito de riesgo generales de la empresa. Como parte de las actividades de gobierno sobre los riesgos, se define el apetito por el riesgo de la empresa, debiendo éste quedar reflejado en las políticas. Una empresa con aversión al riesgo tendrá diferentes políticas que una organización que asuma riesgos. Esto se debe a la naturaleza de la empresa, el entorno en el que opera y su actitud hacia el riesgo.

Las políticas deberían tener en cuenta la situación específica en la que empresa exista. El contenido de las políticas de la empresa cambiará dependiendo del contexto de la organización y del entorno en el que opera. Esta situación específica está compuesta de factores tales como:
- Regulaciones aplicables únicamente a la empresa
- Requisitos de negocio operativos y funcionales
- Necesidades de propiedad intelectual y protección de datos competitivos
- Políticas existentes de alto nivel y la cultura corporativa
- Diseños únicos de arquitectura TI de la empresa
- Regulaciones gubernamentales tales como la Ley Federal de Seguridad de la Información (Federal Information Security Management Act, FISMA) en los Estados Unidos
- Estándares de la industria (PCI DSS)

En la guía detallada, se hacen algunas propuestas sobre el posible contenido de una política de seguridad de la información:
- Cobertura dentro de la empresa
- Presupuesto y gestión de costes del ciclo de vida de la seguridad de la información
- Planes estratégicos y gestión de cartera de la seguridad de la información
- Visión, metas y métricas
- Innovación y buenas prácticas
- Creación de valor
- Comunicación e información a las partes interesadas
- Gobierno de la tecnología y la arquitectura
- Cultura y concienciación en seguridad de la información
- Propiedad atribuida a las partes interesadas relevantes sobre la información crítica
- Proveedores y terceros

Esta lista puede proporcionar una guía para desarrollar una política única adaptada y alineada a la situación específica. La política puede existir en un documento amplio que contenga todos los elementos relevantes o en un documento de guía que contenga una directriz con enlaces a políticas más detalladas. Las dos opciones son aceptables siempre y cuando el formato se describa claramente en el marco de políticas.

2.5 Ciclo de Vida de las Políticas

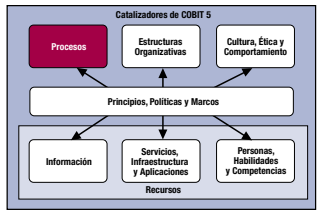
Según se define en APO1.03 *Mantener los catalizadores del sistema de gestión*, las políticas necesitan ser gestionadas a lo largo de su ciclo de vida. Se requiere una evaluación y actualización de las políticas de forma regular, y también debería implantarse un mecanismo desencadenante de actualizaciones fuera del ciclo de vida.

La evolución y la tecnología emergente en las políticas:
La evolución del uso de los dispositivos móviles, las redes sociales, computación en la nube, aplicaciones departamentales o el uso del negocio de TI no centralizado deberían desencadenar la necesidad de revisar y actualizar una política. Además, los cambios en los requerimientos de cumplimiento de regulaciones locales necesitan una revisión y actualización de las políticas existentes, o quizás la necesidad de nuevas políticas.

Además, en muchas empresas se requiere una revisión de las políticas fuera de la función de seguridad de la información. Los potenciales problemas de privacidad, por ejemplo, pueden desencadenar la participación de las funciones de asesoría jurídica y recursos humanos en la aprobación de las políticas. La ISSC sigue siendo responsable en última instancia del desarrollo de las políticas y su actualización. Este comité de supervisión puede requerir la aprobación de la dirección ejecutiva cuando se adapte toda la política de la seguridad de la información. Para las políticas más técnicas, el comité de supervisión puede decidir independientemente. En compañías más pequeñas, pueden existir políticas aunque no estén documentadas o formalmente aprobadas.

Página dejada en blanco intencionadamente

Capítulo 3
Catalizador: Procesos



Este capítulo contiene todos los procesos de COBIT 5 creados específicamente para seguridad de la información, incluyendo detalles como metas y métricas de seguridad de la información y actividades específicas de seguridad de la información. El contenido del proceso de COBIT 5 se reduce a lo que es relevante para seguridad de la información y se extiende para alinearse con fuentes externas de seguridad de la información.
De por sí, esta es una información específica de seguridad complementaria a la publicación *COBIT 5: Procesos Catalizadores.*

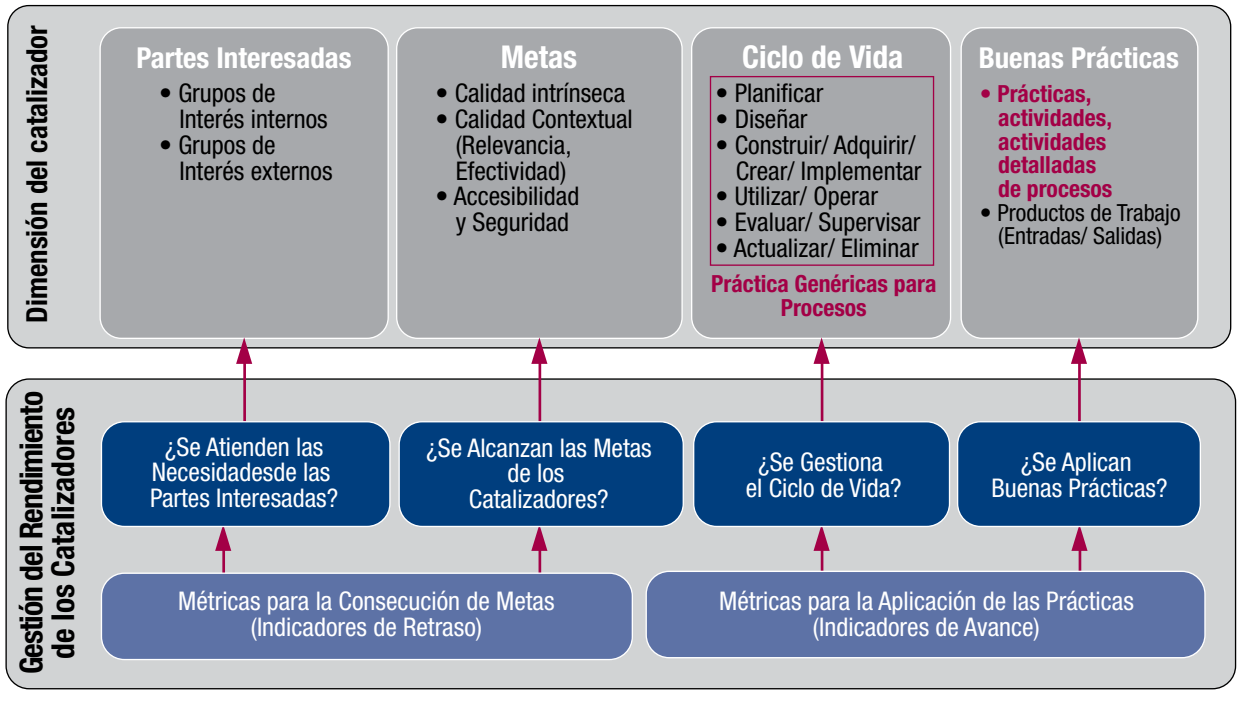
Los siguientes elementos serán analizados:
1. El modelo de proceso
2. Los procesos de gobierno y gestión
3. Los procesos de gobierno y gestión de seguridad de la información
4. Relación de los procesos con otros catalizadores

Los procesos describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de salidas como apoyo para alcanzar el total de las metas relacionadas con TI, como se describió anteriormente.

3.1 El Modelo de Procesos

La **figura 11** muestra los diferentes componentes de un proceso como se define dentro de *COBIT 5 para Seguridad de la Información* a alto nivel.

Figura 11—Catalizador de Cobit 5: Proceso



Este modelo de proceso es una extensión del modelo de catalizador genérico explicado en la **figura 8.** COBIT 5 defines a process as **'una colección de prácticas influidas por las políticas y procedimientos de empresa que toma entradas de varias fuentes (incluyendo otros procesos), manipula las entradas y produce salidas (p. ej., productos, servicios)'**. El modelo de proceso muestra:

- Los procesos tienen **partes interesadas**, internas (p.ej. Consejo de Administración, la dirección, el personal, los voluntarios, entidades reguladoras) y externas (p.ej. clientes, socios comerciales, accionistas) cada una con sus propios roles; las partes interesadas y sus niveles de responsabilidad (documentados en matrices [RACI] que muestran quién realiza, quién es responsable, a quién se consulta o a quién se informa).

  Las metas del proceso se pueden categorizar en metas intrínsecas, metas contextuales, y metas de accesibilidad y seguridad. En cada nivel de la cascada de metas se definen métricas para medir hasta qué punto dichas metas son alcanzadas.

Adicionalmente, un segundo aspecto de la gestión del rendimiento del catalizador describe el grado al que se aplicaron las buenas prácticas. Aquí también se pueden definir métricas asociadas para ayudar a la gestión del catalizador.
- Cada proceso tiene un **ciclo de vida** que incluye que el proceso se define, crea, opera, supervisa y ajusta/actualiza o retira. Las prácticas de procesos genéricos como las definidas en el modelo de evaluación de procesos COBIT [1] basado en ISO/IEC 15504 pueden ayudar en los procesos de definición, ejecución, supervisión y optimización.
- **Las buenas prácticas internas** se describen en un nivel creciente de detalle: prácticas, actividades y actividades detalladas**. Las buenas prácticas externas** pueden existir en cualquier forma o nivel de detalle, y la mayoría de las veces hacen referencia a otros estándares y marcos. Los usuarios pueden referirse a estas buenas prácticas externas en todo momento, sabiendo que *COBIT 5 para Seguridad de la Información* está alineado con estos estándares cuando es pertinente y se proporcionará información de mapeo.

La alineación entre *COBIT 5 para Seguridad de la Información* y otros estándares y modelos se describe más detalladamente en la sección III de esta publicación.

La información detallada de gobierno y gestión de COBIT 5 relacionada con los procesos y específica de seguridad de la información incluye:
- **Identificación del proceso**—En la primera página de cada descripción de proceso, se identifica la siguiente información:
  - Etiqueta de proceso—Consiste en el prefijo del dominio (EDM, APO, BAI, DSS, MEA) y el número de proceso
  - Nombre del proceso—Breve descripción, indicando el asunto principal del proceso.
  - Área—Gobierno o gestión
  - Nombre de Dominio
- **Descripción del proceso**—Este párrafo corto describe el proceso en más detalle y contiene una:
  - Visión general de lo que hace el proceso, p.ej. el propósito del proceso.
  - Visión a alto nivel de cómo el proceso lleva a cabo su propósito
- **Declaración del propósito del proceso**—Una descripción del propósito general del proceso
- **Metas y métricas del proceso**—Para cada proceso, se incluyen un número limitado de metas del proceso **específicas de seguridad de la información**, y por cada meta del proceso se indican un limitado número de ejemplos de métricas específicas de seguridad de la información, reflejando la clara relación entre metas y métricas.
- **Información detallada de las prácticas de proceso**—Este descripción contiene, para cada práctica:
  - Título y descripción de la práctica.
  - Entradas y salidas (resultados del trabajo) **específicas de la práctica de seguridad de la información**, con indicaciones de origen y destino.
  - Actividades del proceso **específicas de seguridad de la información**

3.2 Procesos de Gobierno y Gestión

Como se ha mencionado anteriormente, uno de los principios rectores de COBIT 5 es la distinción que se realiza entre el gobierno y la gestión. En línea con este principio, se espera que la empresa implemente varios procesos de gobierno y varios procesos de gestión para proporcionar un gobierno y una gestión integral de la seguridad de la información.

Al considerar los procesos de gobierno y gestión en el contexto empresarial, la diferencia entre los dos tipos de procesos reside en los objetivos de los mismos:
- **Procesos de gobierno**—Los procesos de gobierno se ocupan de los objetivos de gobierno de las partes interesadas – proporcionar valor, optimizar riesgos y recursos. Incluyen prácticas y actividades enfocadas a evaluar opciones estratégicas, proporcionando dirección a seguridad de la información y supervisando sus resultados (como se define en el dominio de COBIT 5 Evaluar, Orientar y Supervisar [EDM] , en línea con los conceptos del estándar ISO/IEC 38500).
- **Procesos de gestión**—Estos procesos incluyen prácticas y actividades orientados a cubrir las áreas de responsabilidad de planificar, construir, ejecutar y supervisar *(Plan, Build, Run and Monitor - PBRM*) la seguridad de la información. La gestión de procesos proporciona cobertura extremo a extremo de la seguridad de la información.

Los resultados de los dos tipos de procesos son diferentes y están destinados a audiencias diferentes. Sin embargo, internamente, todos los procesos requieren actividades de planificación, construcción o implementación, ejecución y supervisión del proceso en sí mismo.

3.3 Procesos de Gobierno y Gestión de Seguridad de la Información

La **figura 7** muestra el conjunto completo de los 37 procesos de gobierno y gestión de COBIT 5. Los detalles de todos los procesos específicos de seguridad de la información, de acuerdo con el modelo de procesos descrito previamente, se incluyen en el **apéndice B.**

[1] ISACA, *COBIT® Modelo de Evaluación de Procesos (PAM): Usando COBIT 4,1,* EE.UU., 2011, *www.isaca.org/cobit-pam*

3.4 Relación de los Procesos con Otros Catalizadores

Como se describe en la sección I, todos los catalizadores están interconectados e interactúan dinámicamente; por ejemplo: para alcanzar los principales objetivos de la empresa, la empresa debe considerar siempre un conjunto interconectado de catalizadores. Por lo tanto, cada catalizador:

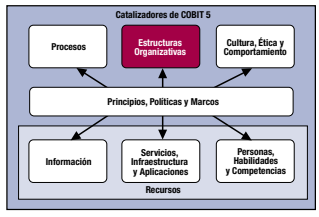
- Necesita la entrada de otros catalizadores para ser completamente efectivo (p.ej.: los procesos necesitan información, las estructuras organizativas necesitan de habilidades y comportamientos).
- Entrega la salida para beneficio de otros catalizadores (p.ej: los procesos entregan información, las habilidades y los comportamientos hacen eficientes a los procesos).

Para cada proceso, se provee de una caja al final de la descripción del proceso, describiendo los catalizadores relacionados, como en el ejemplo siguiente:

> Para más información sobre los catalizadores relacionados, por favor consulte:
> • Apéndice D. Guía detallada: Cultura, Ética y Comportamiento.

Página dejada en blanco intencionadamente

Capítulo 4
Catalizador: Estructuras Organizativas

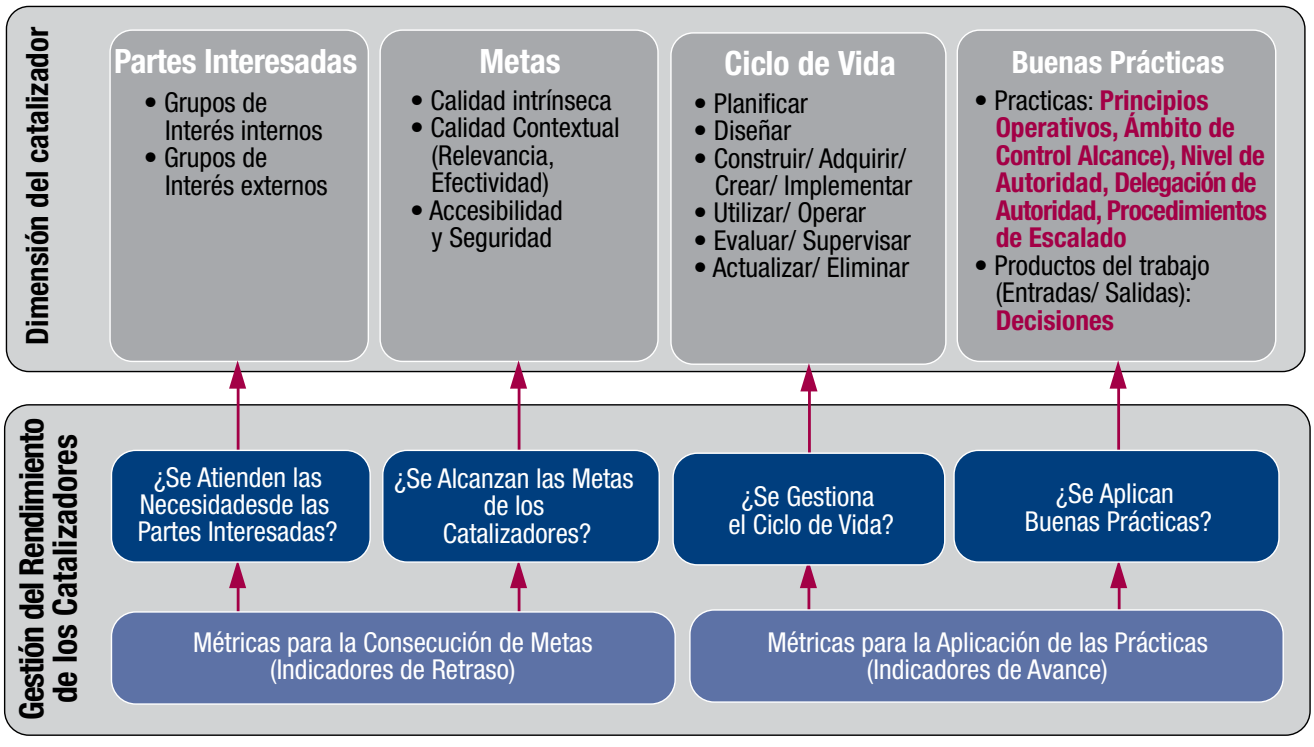


Este capítulo discute las estructuras organizativas relevantes para seguridad de la información. Las estructuras organizativas son los elementos clave en la toma de decisiones de una empresa. Se cubren los siguientes elementos:
1. El modelo de estructuras organizativas.
2. Ejemplos de roles y estructuras de seguridad de la información que se suelen encontrar.
3. Responsabilidad sobre la seguridad de la información dentro de la empresa.

4.1 Modelo de Estructuras Organizativas

Las estructuras organizativas se definen como los elementos clave en la toma de decisiones de una empresa. Estas entidades se pueden estructurar de acuerdo a las dimensiones ilustradas en el modelo de catalizadores mostrado en la **figura 12**.

Figura 12—Catalizador de COBIT 5: Estructuras Organizativa



La **figura 12** muestra a un alto nivel los diferentes componentes de la estructura organizativa tal y como se define en esta publicación. El modelo de proceso es una extensión del modelo de catalizadores genéricos explicado en la **figura 8**.

El modelo de estructuras organizativas indica que:
- Los roles de las **partes interesadas** de las estructuras organizativas (que incluyen la toma de decisiones, influenciar y asesorar) varían, según lo hagan las partes (p.ej.: el interés que tengan en las decisiones tomadas por la estructura).
- **Las metas** para el propio catalizador de las estructuras organizativas deberían incluir un mandato adecuado, principios operativos bien definidos y la aplicación de otras buenas prácticas. El resultado del catalizador de las estructuras organizativas debería incluir varias actividades y buenas decisiones.
- Una estructura organizativa tiene un **ciclo de vida**. Es creada, existe y es ajustada y, finalmente, puede ser disuelta. Durante su creación, se debe definir un mandato –una razón y un propósito para su existencia.
- Se pueden distinguir varias **buenas prácticas** para las estructuras organizativas, que se describen en detalle en el **apéndice C**.

Las partes interesadas son el primer componente en el modelo catalizador de las estructuras organizativas. Desde un punto de vista de seguridad de la información, las partes interesadas se organizan en dos categorías:
- Roles y estructuras **específicas** de seguridad de la información—Estos roles y estructuras son internas a la función de seguridad de la información.
- Roles y estructuras **relacionadas** con seguridad de la información—Estos roles y estructuras no están organizados u ocupados por miembros de la función de seguridad de la información, pero estos roles y estructuras discuten o manejan problemas o asuntos de seguridad de la información (p.ej.: propietarios de procesos de negocio y usuarios).

4.2 Roles y Estructuras de Seguridad de la Información

Dentro de una empresa normal, se suelen encontrar los roles y estructuras de seguridad de la información descritos en la **figura 13**, filas 1, 2 y 3.

Figura 13—Roles/Estructuras Específicas de Seguridad de la Información

Rol/Estructura	Mandato
Director de Seguridad de la Información (CISO) (definido en COBIT 5)	Toda la información del programa de seguridad de la información de la empresa
Comité de supervisión de seguridad de la información (ISSC)	Comprobar mediante la monitorización y revisión que las buenas prácticas en seguridad de la información se aplican eficiente y consistentemente a lo largo de toda la empresa.
Gerente de seguridad de la información (ISM) (definido en COBIT 5)	Responsabilidad general para la gestión de esfuerzos en seguridad de la información
Comité de Gestión de Riesgos Corporativos (ERM)	Es el responsable de la toma de decisiones en la empresa para evaluar, controlar, optimizar, financiar y monitorizar el riesgo de todos los orígenes con el propósito de incrementar el valor de la empresa a corto y largo plazo para las partes interesadas.
Custodios de la información/propietarios del negocio	Es el enlace entre el negocio y las funciones de seguridad de la información

En el **apéndice C**, se encuentran las descripciones detalladas de estos grupos y roles. Para cada uno de ellos, se han descrito las siguientes buenas prácticas:
- **Composición**—Se deberían requerir un conjunto apropiado de competencias para todos los miembros del grupo organizativo.
- **Mandato, principios operativos, alcance del control y nivel de autorización**—Estos elementos describen los acuerdos prácticos de como operará la estructura, los límites de los derechos de decisión de la estructura organizativa, las responsabilidades y la ruta de escalado o las acciones necesarias en caso de problemas.
- **Matriz RACI a alto nivel**—Las matrices RACI vinculan actividades de procesos con estructuras organizativas y/o roles individuales en la empresa. Estas tablas describen el nivel de involucración de cada rol para cada práctica del proceso: (R) Responsable de hacer, (A) Responsable de que se haga, (C) Consultado o (I) Informado.
- **Entradas/Salidas**—Una estructura requiere entradas (normalmente información) antes de que pueda tomar decisiones informadas y, asimismo, produce salidas, por ejemplo, decisiones, otra información o solicitudes de entradas adicionales.

Dependiendo de la empresa, se pueden crear roles específicos de seguridad de la información adicionales. Ejemplos de roles típicos en un equipo de seguridad de la información son:
- Administradores de seguridad de la información.
- Arquitectos de seguridad de la información.
- Oficiales de cumplimiento y auditorias de seguridad de la información.

En empresas pequeñas, sin embargo, las tareas cubiertas por estos roles pueden recaer en el gerente de seguridad de la información. Adicionalmente a los roles y estructuras específicos de seguridad de la información, en las últimas dos filas de la **figura 13** se muestran dos ejemplos de estructuras relacionadas.

Se puede encontrar una guía práctica adicional sobre estas estructuras en el **apéndice C**.

Estos roles y estructuras son apropiados para una empresa que no solo maneje información sensible, sino que también haya alcanzado un cierto tamaño y complejidad organizativa. Para empresas más grandes o empresas que necesitan un foco más fuerte en seguridad de la información, es necesaria una organización de seguridad de la información más elaborada, y se pueden añadir grupos y roles adicionales.

Se debe prestar especial atención a la relación existente entre seguridad de la información y la TI dentro de las empresas. Es los casos en los que seguridad de la información informa directamente a TI, puede existir un conflicto de intereses. TI, por su naturaleza, ofrece un servicio a la empresa, mientras que seguridad de la información gestiona el riesgo relacionado con la protección de la información. Esta dicotomía puede llevar a TI a ignorar prácticas de seguridad de la información anteponiendo el servicio al cliente. Por lo tanto, se debería establecer un cierto grado de independencia entre TI y seguridad de la información.

4.3 Responsabilidad Sobre la Seguridad de la Información

Es importante tener en cuenta que la posición de la(s) función(es) de seguridad de la información en la empresa es un factor clave para determinar la capacidad de la organización para proteger la información. Esta posición puede ser la diferencia entre una seguridad de la información alineada de forma proactiva con las iniciativas empresariales y aquella que solo es una idea de último momento para mitigar el riesgo, con opciones limitadas para el tratamiento del riesgo.

El consejo de dirección tiene la responsabilidad final de todos los temas, incluyendo la seguridad de la información. Esta responsabilidad puede y debe ser delegada en el nivel adecuado dentro de la empresa. Teniendo en cuenta que la seguridad de la información es una cuestión crítica para el negocio, la organización siempre debe asignar la responsabilidad final sobre la seguridad de la información a un alto miembro de la dirección ejecutiva. De no hacerlo, se puede exponer al consejo directivo a las reclamaciones por negligencia por parte de los reguladores o de otros grupos de interés, en caso de que ocurra un incidente.

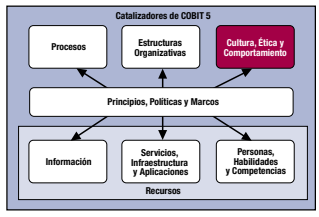
La decisión de delegar la responsabilidad de manera general depende de la situación específica de la empresa. La **figura 14** contiene algunas posibles ventajas y desventajas de que seguridad de la información reporte a un determinado rol, que se pueden tener en cuenta para tomar la decisión.

Figura 14—Ventajas y Desventajas de Posibles Caminos para el Reporte sobre la Seguridad de la Información

Roles	Ventajas	Desventajas
Director General Ejecutivo (CEO)	El riesgo de información es elevado al más alto nivel dentro de la empresa.	Los riesgos de información necesitan ser presentados en un formato que sea comprensible para el CEO. Dada la multitud de responsabilidades del CEO, el riesgo de la información podría ser monitorizado y administrado en un nivel demasiado alto de abstracción o no puede ser plenamente entendido en sus detalles relevantes.
Director de Informática y Sistemas (CIO)	Los temas de seguridad de la información y soluciones pueden ser alineadas con todas las iniciativas de TI.	Los riesgos de información no se pueden tratados debido a que otras iniciativas de TI tienen prioridad sobre la seguridad de la información. Existe un conflicto de intereses. El trabajo realizado por los profesionales de seguridad de la información puede estar focalizado en TI y no focalizado en seguridad de la información. En otras palabras, puede haber un enfoque insuficiente en el negocio.
Director General Financiero (CFO)	Los temas de seguridad de la información pueden ser direccionados desde un punto de vista de impacto económico en el negocio.	Los Riesgos de la información no pueden ser tratados debido a que los plazos de las iniciativas financieras tienen prioridad sobre seguridad de la información. Existe un posible conflicto de interés.
Director General de Riesgos (CRO)	El riesgo de información es elevado a una posición que puede mirarse como un riesgo con perspectiva de estrategia, financiero, operacional, reputacional o de cumplimiento.	Esta función no existe en la mayoría de las empresas. A menudo se encuentra dentro de los servicios financieros. En empresas en las cuales el CRO no existe, las decisiones de riesgo pueden ser tomadas por el CEO o el Consejo de Administración.
Director General de Tecnología (CTO)	La seguridad de la información puede ser asociada y se incluirá en los futuros planes de trabajo de tecnología.	Los riesgos de información no pueden ser tratados debido a que la tecnología prevalece sobre la seguridad de la información.
Director General Operativo (COO)	Los problemas de seguridad de información y soluciones pueden ser abordados desde el punto de vista del impacto en el negocio "operaciones.	Los riesgos de información no pueden ser tratados debido a que las iniciativas de operaciones y plazos prevalecen sobre la seguridad de la información.
Consejo de administración	El riesgo de información es elevado al más alto nivel dentro de la empresa.	Los riesgos de información tienen que ser presentados en un formato que sea entendible por los miembros del consejo, y por lo tanto puede ser un nivel demasiado alto para ser relevante.

Página dejada en blanco intencionadamente

Capítulo 5
Catalizadores: Cultura, Ética y Comportamiento

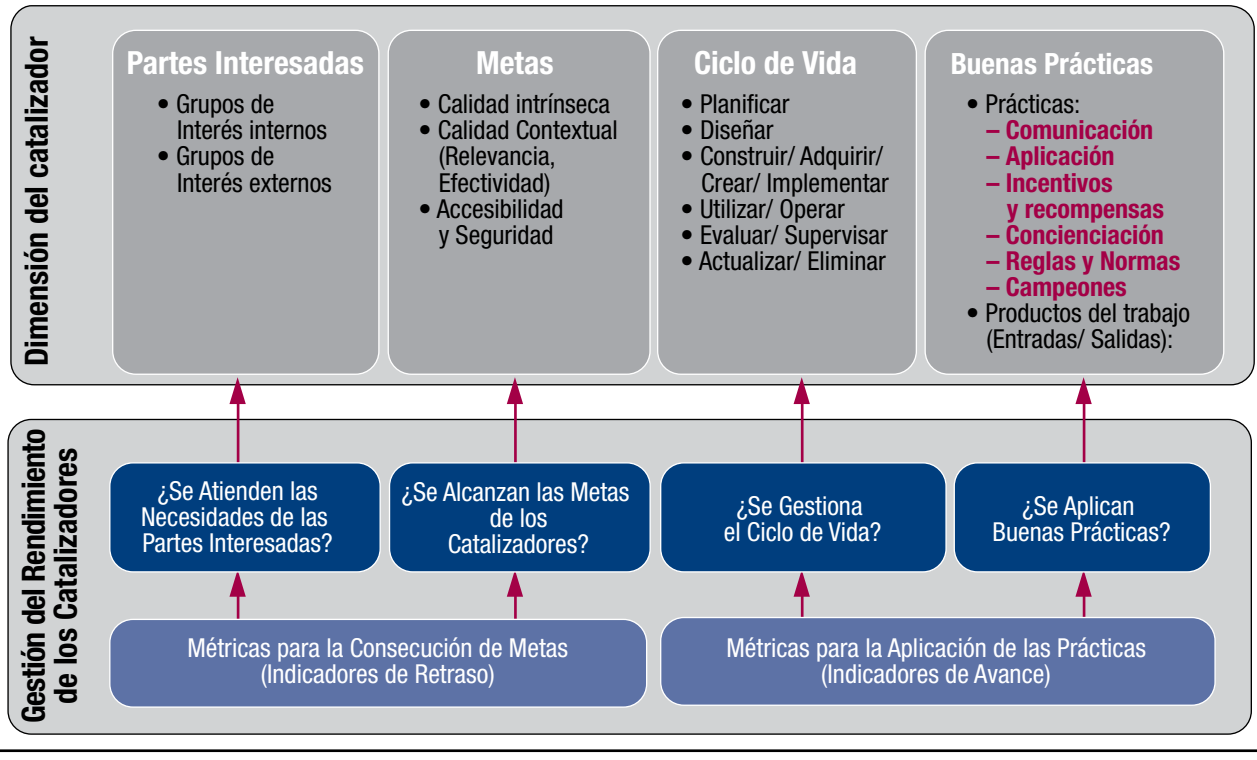


El Comportamiento de los individuos y de las empresas es a menudo subestimado como factor de éxito en el gobierno y la gestión de la seguridad de la información. En este capítulo se cubren los siguientes elementos:
1. El modelo cultural
2. El ciclo de vida de la cultura
3. Liderazgo y campeones que pueden influir en el comportamiento.
4. El comportamiento deseable que debería ser fomentado dentro de cualquier empresa.

5.1 Modelo Cultural

La cultura, la ética y el comportamiento se pueden estructurar de acuerdo a las dimensiones que aparecen en la **figura 15**.

Figura 15—Catalizador COBIT 5: Cultura, Ética y Comportamiento



La **figura 15** muestra los diferentes componentes de la cultura, la ética y el comportamiento tal y como se definen en esta publicación. Este modelo de proceso es una extensión del modelo de catalizadores genérico explicado en la **figura 8**.

El modelo de la cultura, la ética y el comportamiento indica que:
- Los grupos de interés en la cultura, la ética y el comportamiento abarcan toda la empresa, incluso trascienden a grupos de interés externos como los reguladores, auditores externos y organismos de supervisión. Los intereses son dobles: algunos grupos de interés, por ejemplo, juristas, gestores de riesgos, gestores de recursos humanos, directores financieros, se ocupan de la definición, ejecución y hacer cumplir los comportamientos deseados, mientras que otros tiene que alinearse con las reglas y normas ya definidas. Por consiguiente, cuando hay que influir en la cultura, los dos grupos de interés deben tenerse en cuenta. Por ejemplo, no sólo el personal interno debe ser consciente de la situación de la seguridad de la información, sino también lo deben ser los consultores externos, proveedores y otras partes externas.
- Los **objetivos** de este catalizador se relacionan con la ética de la organización (determinada por los valores que la empresa quiere vivir), la ética individual (determinada por los valores personales de cada individuo en la empresa) y los comportamientos individuales.
- Las culturas organizativas, la postura ética, los comportamientos individuales, etc. tienen **ciclos de vida**. A partir de la cultura existente, una empresa puede identificar los cambios necesarios y trabajar para que se lleven a cabo. Hay varias herramientas- descritas como buenas prácticas- que pueden ser usadas.

- **Buenas prácticas** para crear, fomentar y mantener un comportamiento deseado en toda la empresa incluyen:
  – La comunicación a toda la empresa de los comportamientos deseados y de los valores corporativos fundamentales
  – Conocimiento de la conducta deseada (reforzado por el comportamiento ejemplar de la alta dirección y otros líderes)
  – Incentivos para alentar y medidas disuasorias para hacer cumplir las actitudes, normas y reglas (que proporcionan una mayor orientación sobre los comportamientos deseados y relacionan muy claramente con los principios y políticas).

El comportamiento humano es uno de los factores claves que determinan el éxito de cualquier empresa. Los comportamientos de todos los miembros de la empresa determinan colectivamente la cultura de la empresa. Muchos factores dirigen el comportamiento: factores externos tales como las creencias, el origen étnico, el nivel socio económico, la ubicación geográfica, las experiencias personales y las relaciones interpersonales en las empresas, los objetivos y las ambiciones personales.

La cultura se define en BMIS[2] como "un patrón de comportamientos, creencias, suposiciones, actitudes y formas de hacer las cosas". La publicación de ISACA *Creando la Cultura de la Seguridad de la Información*[3] amplía el liderazgo de pensamiento en torno a la cultura y la seguridad de la información y describe la cultura de la seguridad de la información como:

> *Todas las empresas tienen una cultura en seguridad de la información. En la mayoría de los casos, carece de intencionalidad y es inconsistente a las medidas que existen; en otros, es robusta y guía las actividades diarias de los empleados y otras personas que entran en contacto con la empresa.*

5.2 Ciclo de Vida de la Cultura

Como la cultura trasciende a la empresa, evoluciona en el tiempo. Los comportamientos se adaptan, y la conciencia cultural sobre la seguridad de la información puede aumentar o disminuir. Es importante entender la cultura existente, para que los cambios positivos permitan alcanzar una cultura de la seguridad. Existen muchas metodologías de medición de la cultura. Además de la medir la cultura empresarial, la eficacia de las medidas de seguridad de la información debería ser medida para evaluar la cultura de la seguridad subyacente.

Para tener una visión correcta de la cultura de la seguridad de la información, el comportamiento de las partes interesadas se debe medir en el tiempo. Ejemplos de tales mediciones incluyen:
- Calidad de las contraseñas
- Uso de tarjetas magnéticas
- Número de candados para portátiles distribuidos y utilizados por los empleados
- Debates públicos con información confidencial
- Falta de enfoque de la seguridad (contraseñas compartidas, accesos físicos aprovechando las credenciales de la persona autorizada, etc.)
- Protección de la contraseña del usuario en la práctica
- Adhesión a las prácticas de gestión de cambios en aplicaciones y sistemas
- Cumplimentación de los registros de visitantes y responsabilidad de los visitantes
- Porcentaje de etiquetado y marcado correcto de la información (electrónica e impresa)

Como datos estáticos, estos indicadores tienen poco valor. Solo cuando se examina su evolución a lo largo del tiempo pueden proporcionar estas métricas simples un mecanismo solido de evaluación de la cultura de la seguridad de la información.

5.3 Líderes y Campeones

Para influir en la cultura, la empresa necesita líderes para llevar a cabo los cambios en toda la empresa. Los líderes son esas personas de la empresa que están dispuestas a hablar y servir de ejemplo para otros. Los líderes pueden ser los altos ejecutivos de una empresa, pero la actividad no se limita solo a ese grupo dentro de la organización. Los miembros del personal también pueden ser líderes mientras que proporcionan activamente el soportes para el cambio y la aplicación de la cultura. *Crear una Cultura de la Seguridad de la Información* ofrece varios candidatos que pueden servir como líderes de la seguridad de la información.
- Gestores de Riesgos
- Profesionales de la seguridad de la información
- Ejecutivos de alto nivel: CEO, COO, CFO, CIO
- Director de Recursos Humanos

[2] ISACA, *The Business Model for Information Security* (BMIS), EE.UU., 2010
[3] ISACA, *Creating a Culture of Security*, EE.UU., 2011

El liderazgo – los que toman las decisiones – en este contexto de seguridad de la información puede ser igual de importante. Los líderes son necesarios para influir en que la toma de decisiones tenga en consideración los requisitos de seguridad de la información. Es obvio que el liderazgo y los líderes se pueden solapar; sin embargo, ambos se mencionan en diferente contexto. El liderazgo se categoriza como:
- Dirección ejecutiva
- Dirección del negocio
- CISO/ISM

5.4 Comportamiento Deseable

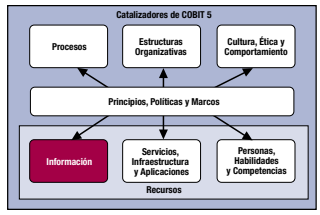
Se han identificado varios comportamientos deseables que influyen positivamente hacia una cultura de seguridad de la información y su implementación en el día a día. Estos incluyen:
- La seguridad de la información se pone en práctica en las operaciones diarias.
- Las personas respetan la importancia de las políticas y los principios de seguridad de la información.
- A las personas se les proporcionan directrices suficientes y detalladas sobre seguridad de la información; además, se fomenta su participación activa en el cambio de la situación actual de la seguridad de la información.
- Todo el mundo es responsable de la protección de la información en la empresa.
- Las partes interesadas saben cómo identificar y dar respuesta a las amenazas de la empresa.
- La dirección soporta proactivamente y anticipa nuevas innovaciones en seguridad de la información y lo comunica a la empresa. La empresa es receptiva para reconocer y gestionar los nuevos retos de seguridad de la información.
- La dirección del negocio entabla colaboraciones continuas con otras funciones que tiene en cuenta la eficacia y la eficiencia de los programas de seguridad de la información.
- La dirección ejecutiva reconoce el valor de la seguridad de la información para el negocio.

Para cada uno de los comportamientos deseables identificados, los siguientes atributos son descritos en el **Apéndice D**:
- **Ética organizativa**—Determinada por los valores que la empresa quiere vivir.
- **Ética individual**—Determinada por los valores de cada individuo de la empresa que, en gran medida, están influidos por valores externos como las creencias, el grupo étnico, la localización geográfica, la historia socio-económica y las experiencias personales.
- **Liderazgo**—Las maneras en las que el liderazgo puede influir sobre el comportamiento deseable:
  – Cómo la comunicación, la aplicación de las reglas y las normas pueden ser utilizadas para influir en el comportamiento
  – La influencia sobre el comportamiento a través del uso de incentivos y recompensas
  – Crear conciencia

Para una información más detallada sobre la cultura de seguridad de la información pueden consultarse BMIS y *"Creating a Culture of Information Security"* en *www.isaca.org.*

Página dejada en blanco intencionadamente

Capítulo 6
Catalizador: Información



Este capítulo contiene directrices sobre cómo la información subyacente a la organización puede ser utilizada para gobernar y gestionar la seguridad de la información en la empresa. Se analizarán los siguientes elementos:

1. El modelo de información
2. Ejemplos de tipos comunes de información
3. Los grupos de interés de la información y cómo identificar las partes que están implicadas dentro de la empresa
4. El ciclo de vida de la información, describiendo las diferentes fases de la gestión de la información en este contexto

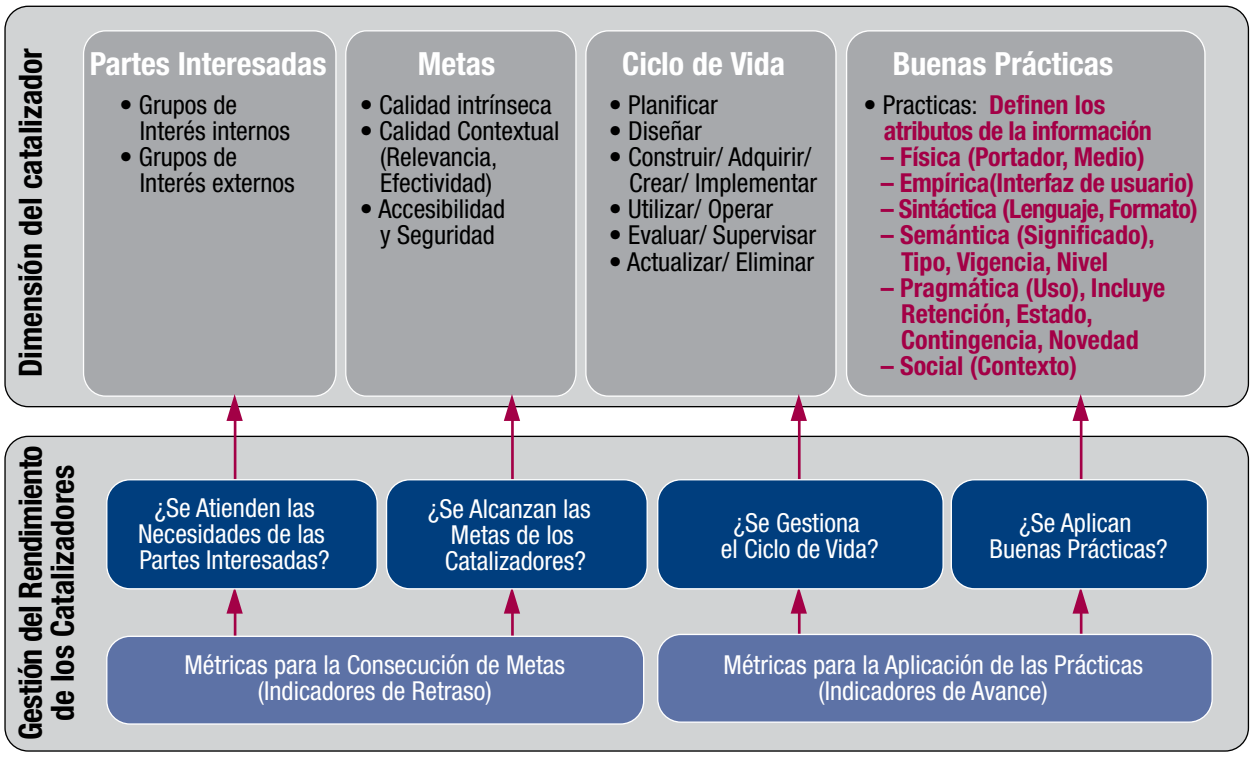
El uso de la información está generalizado en todas las empresas y se requiere para mantenerlas operativas y bien gobernadas. En el nivel operacional, la información es frecuentemente el producto clave de la empresa.

6.1 Modelo de Información

La información (y, como consecuencia, la comunicación) no es solo el principal objeto de la seguridad de la información, sino que se trata además, de un catalizador clave para la seguridad de la información. La información como catalizador de la seguridad de la información significa que la dirección puede utilizar la información como base de la toma de decisiones (por ejemplo, el ISSC puede utilizar el perfil de seguridad de la información para desarrollar una estrategia de seguridad de la información).

La **figura 16** muestra a alto nivel los diferentes componentes de la información, tal y como están definidos en esta publicación. Este modelo de proceso es una extensión del modelo de catalizadores genérico explicado en la **figura 8**.

Figura 16—Catalizador de COBIT 5: Información



El modelo de información indica que:

- Deben identificarse las **partes interesadas** internas y externas y sus áreas clave de responsabilidad; por ejemplo, debe estar claro por qué se preocupan o están interesados en la información.
- Las **metas** de la información están divididas en tres sub-dimensiones de calidad:
  - **Calidad intrínseca**—Extremo hasta el que los valores en relación a los datos son conformes con los valores actuales o reales
  - **Calidad contextual y de representatividad**—Punto hasta el que la información es aplicable a los usuarios y es presentada de forma inteligible y clara, reconociendo que la calidad de la información depende del contexto en el que se usa
  - **Calidad de seguridad / accesibilidad**—Extremo hasta el que la información está disponible o se puede obtener

- El **ciclo de vida completo** de la información debe ser considerado y pueden ser necesarias diferentes aproximaciones durante las diferentes fases del ciclo de vida (planificar, diseñar, construir/adquirir, usar / operar, supervisar y eliminar).
- Las **buenas prácticas** consideran que la información consta de seis capas, presentando de forma continua los atributos de la información, desde el uso en el mundo físico, donde los atributos son enlazados con las tecnologías y los medios para capturar, almacenar, procesar, distribuir y presentar, hasta el uso en el mundo social para dar sentido a la información ("*sense-making*") y actuar.

6.2 Tipos de Información

La siguiente lista contiene ejemplos de tipos de información que son habituales en el contexto de gobierno y gestión de la seguridad de la información. Estos tipos de información varían desde una estrategia hasta un cuadro de mandos operacional, cada uno de ellos sirviendo a un propósito específico dentro del gobierno y la gestión de la seguridad de la información.

Esta lista no se pretende que sea exhaustiva, pero proporciona una idea de cómo el detalle de seguridad de la información se extiende a través de la empresa. Dependiendo de cada empresa, la lista podría ser más limitada o más extensa.

Ejemplos de estos tipos de información son:
- Estrategia de seguridad de la información
- Presupuesto de seguridad de la información
- Plan de seguridad de la información
- Políticas
- Requisitos de seguridad de la información, que podrían incluir:
  - Requisitos de configuración de la seguridad
  - Requisitos de seguridad de la información en los acuerdos a nivel de servicio (SLA) y en los acuerdos a nivel operacional (OLA)
- Material para la concienciación
- Informes de revisión de seguridad de la información, que podrían incluir:
  - Hallazgos de auditorías de seguridad de la información
  - Informes de madurez de seguridad de la información
  - Gestión de riesgos relacionada con la seguridad de la información:
    - Análisis de amenazas
    - Informes de evaluación de vulnerabilidades
- Catálogo de servicios de seguridad de la información
- Información sobre el perfil de riesgo, que incluye:
  - El registro de riesgos
  - Informes de violaciones y pérdidas (informe consolidado de incidentes)
- Cuadro de mando de seguridad de la información (o equivalentes), que incluye:
  - Incidentes de seguridad de la información
  - Problemas de seguridad de la información
  - Métricas de seguridad de la información

Para cada uno de los tipos de información, se proporciona una guía más detallada en el **apéndice E**, incluyendo:
- **Metas**—Descripciones de varias metas a alcanzar, utilizando las tres categorías definidas en el modelo de información
- **Ciclo de vida**—Una descripción especifica de los requisitos del ciclo de vida, además de una aproximación general tal y como se describe en el ciclo de vida de la información en la subsección 6.4 *Ciclo de Vida de la Información*
- **Buenas prácticas** para este tipo de información—Una descripción con contenidos y estructura típicos

6.3 Grupos de interés en la Información

Identificar el grupo de interés en la información es esencial para optimizar el desarrollo y la distribución de la información a través de la empresa. Esta subsección proporciona una aproximación para resumir los emisores y los destinatarios de cada tipo habitual de información.

Por ejemplo, las partes interesadas de la información relacionada con la seguridad de la información en una típica empresa mediana o pequeña (PYME) pueden ser estructuradas como se indica en la **figura 17**, incluyendo:
- Descripción de la parte interesada—Una versión racionalizada de la lista de estructuras genéricas de COBIT 5, complementada con varias partes interesadas externas adicionales para este dominio específico. Esta lista refleja la estructura menos compleja de una PYME, comparada con la de las grandes empresas.

• Tipos de información, tal y como son descritos en la subsección 6.2 Tipos de Información.
• Una indicación de la naturaleza de las relaciones entre las partes interesadas para cada tipo de información:
  – A – Aprobador
  – O – Originador (emisor)
  – I – Informado del tipo de información
  – U – Usuario del tipo de información

Figura 17—Ejemplos de Grupos de Interés para Información Relacionada con Seguridad de la Información (Empresas Pequeñas /Medianas)

Parte Interesada	Tipo de información									
	Estrategia de Seguridad de la Información	Presupuesto de Seguridad de la Información	Plan de Seguridad de la Información	Políticas	Requerimientos de Seguridad de la Información	Material de Concienciación	Informes de Revisión de Seguridad de la Información	Catálogo de Servicios de Seguridad de la Información	Perfil de Riesgo de la Información	Cuadro de Mando de Seguridad de la Información
Interno: Empresa										
Consejo de Administración	U			I		U	I		A	
Director General Ejecutivo (CEO)	U			A		U	I		U	
Director General Financiero (CFO)		A		U		U			U	
Director de Seguridad de la Información (CISO)	O	U	O	O	A	A	A	A	U	U
Comité de Dirección de la Seguridad de la Información (ISSC)	A	O	A	U	U	I	U	I	U	U
Propietario del proceso de negocio				U	O	U		U	U	
Jefe de Recursos Humanos (HR)				U		U				
Interno: TI										
Director Informática/Sistemas (CIO)	U	O	U	U	U	U	I		U	U
Gerente de Seguridad de la Información (ISM)	U	U	U	O	U	O	O	O	O	O
Externo										
Inversores						I				
Aseguradores						I	I		I	
Reguladores		I				I	I			
Socios de Negocio						I	I			
Vendedores/Proveedores						I				
Auditores Externos		I				I	I		I	I

Una plantilla con todos los tipos de información y las partes interesadas potenciales basada en COBIT 5 se proporciona en el **apéndice E**.

6.4 Ciclo de Vida de la Información

Los tipos específicos de información relacionados con la seguridad de la información, tales como los ejemplos proporcionados en la subsección *6.2 Tipos de Información*, están vinculados también a un ciclo de vida. Además, la función de seguridad de la información tiene un importante rol facilitador en este ciclo de vida. Esta dualidad en el contexto de la información (como facilitador del ciclo de vida y como usuario de la información) supone un aumento en la importancia de la seguridad de la información en la empresa.

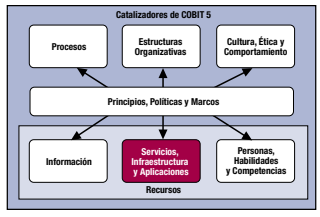
La gestión del conocimiento se describe en el proceso BAI08 de *COBIT 5: Procesos Catalizadores.* Este proceso detalla el ciclo de vida que la información debe seguir para estar segura y eficientemente gestionada en la empresa. El ciclo de vida completo de la información debe ser considerado para asegurar su exactitud y uso óptimo. Adicionalmente, podrían ser necesarias diferentes aproximaciones a la información en diferentes fases del ciclo de vida. Se pueden distinguir las siguientes fases:

- **Planificar/diseñar/construir/adquirir**—La información es identificada, adquirida y clasificada en esta fase. Las actividades en esta fase se pueden referir al desarrollo de estándares y definiciones (p.ej., definiciones de datos o procedimientos de recolección de datos), la creación de registros, la compra de datos o la carga de ficheros externos.
- **Usar/operar**—Esta fase incluye:
  - **Almacenar**—La fase en la cual la información se encuentra electrónicamente o en copia impresa (o incluso en la memoria humana). Las actividades en esta fase se pueden referir al almacenamiento de la información de forma electrónica (por ejemplo, ficheros electrónicos, bases de datos o almacenes de datos) o en copia impresa (por ejemplo, documentos en papel).
  - **Compartir**—La fase en la cual la información se encuentra disponible para su uso a través de un método de distribución. Las actividades en esta fase se pueden referir a los procesos involucrados en obtener la información y ubicarla donde pueda ser accesible y utilizada (p.ej., distribuir documentos vía email). Para la información que se encuentra de forma electrónica, esta fase del ciclo de vida puede solaparse en gran medida con la fase de almacenamiento (por ejemplo, compartir información a través del acceso a bases de datos o a ficheros / documentos en servidores).
  - **Usar**—La fase en la cual la información se utiliza para alcanzar las metas. Las actividades en esta fase se pueden referir a diferentes tipos de uso de la información (p.ej., toma de decisiones gerenciales, ejecutar procesos automatizados), y también pueden incluir actividades como la recuperación de la información o la conversión entre diferentes tipos de formatos de la información.
- **Supervisar**—La fase en la cual se asegura que los recursos de la información continúan trabajando de la forma apropiada (es decir, que la información siga siendo de valor). Las actividades en esta fase se pueden referir al mantenimiento de la información actualizada así como a otro tipo de actividades de gestión de la información (por ejemplo, mejora, depuración, fusión de datos o eliminación de información duplicada en almacenes de datos).
- **Eliminar**—La fase en la cual los recursos de la información se descartan cuando ya no son útiles. Las actividades en esta fase se pueden referir al archivado o la destrucción de la información.

Las fases del ciclo de vida de la información están alineadas con las prácticas del proceso BAI08.

En la guía detallada del **apéndice E** se proporcionan una descripción específica de los requisitos del ciclo de vida y una aproximación general.

Capítulo 7
Catalizador: Servicios, Infraestructuras y Aplicaciones

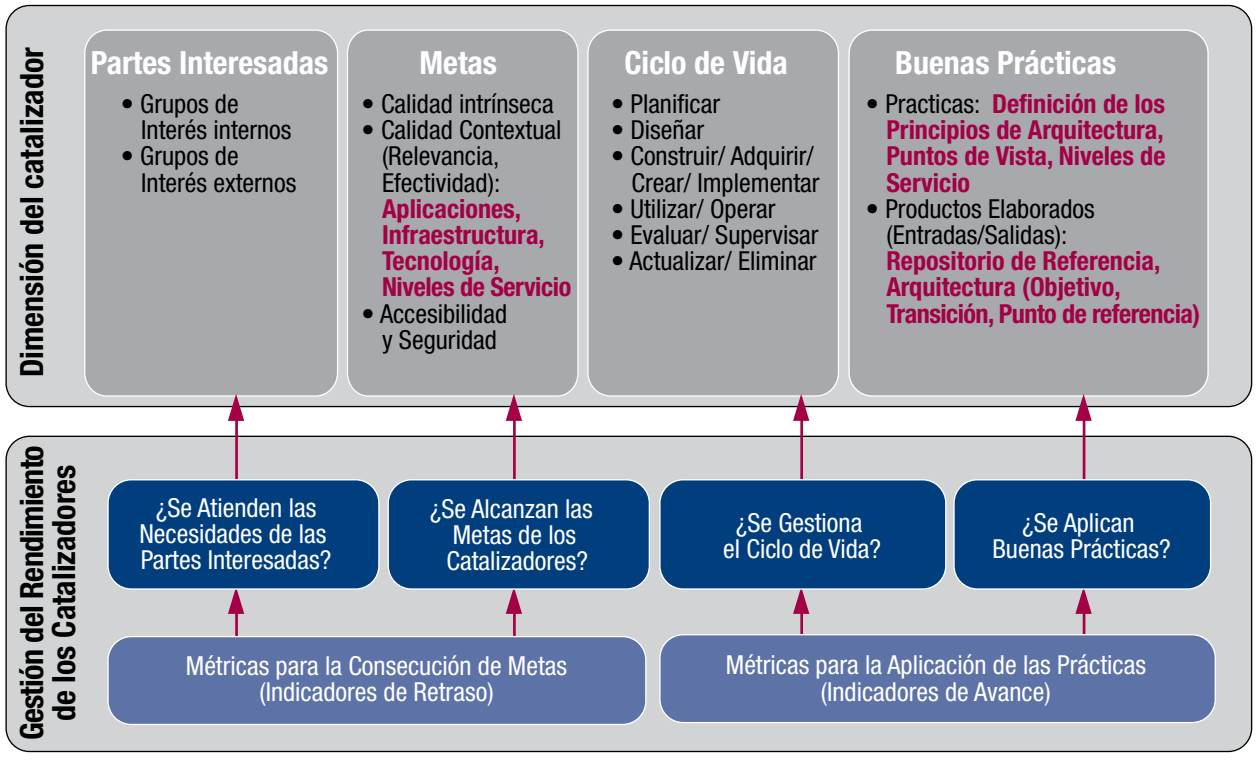


Los servicios, la infraestructura y las aplicaciones proporcionan a la empresa información, procesado de la información y servicios. Los siguientes elementos se cubren en este capítulo:
1. El modelo de servicios, infraestructura y aplicaciones
2. Los servicios, la infraestructura y las aplicaciones de seguridad de la información habituales en las empresas

7.1 Modelo de Servicios, Infraestructuras y Aplicaciones

Los servicios, las infraestructuras y las aplicaciones se pueden estructurar conforme a las dimensiones ilustradas en la **figura 18**.

Figura 18—Catalizador COBIT 5: Servicios, Infraestructuras y Aplicaciones



La **figura 18** muestra a alto nivel los diferentes componentes de servicios, infraestructuras y aplicaciones, tal como se definen en esta publicación. Este modelo de procesos es una extensión del modelo genérico de catalizadores expuesto en la **figura 8**.

El modelo de servicios, infraestructuras y aplicaciones indica que:
- Las **partes interesadas** en las capacidades de servicio (el término que describe conjuntamente a los servicios, las infraestructuras y las aplicaciones) pueden ser internas o externas. Los servicios pueden ser prestados por entidades internas o externas (p.ej., departamentos internos de TI, gerentes de operaciones, proveedores de servicios externos), y los usuarios de servicios también pueden ser internos (p.ej., usuarios de negocio) o externos a la compañía (p.ej., socios, clientes, proveedores). Los intereses de cada una de las partes implicadas deben ser identificados y se centrarán en ofrecer los servicios adecuados o en recibir los servicios solicitados por parte de los proveedores.
- Los **objetivos** de la capacidad a nivel de servicio se expresan en términos de servicios (aplicaciones, infraestructura y tecnología) y niveles de servicio, considerando qué servicios y niveles de servicio son más económicos para la compañía. Una vez más, los objetivos se relacionan con los servicios y con cómo estos son proporcionados, así como con sus resultados, es decir, la contribución a unos procesos de negocio satisfactoriamente sustentados. Esto se describe con mayor detalle en el **apéndice F**.
- Las capacidades de servicio tienen un **ciclo de vida**. Las capacidades de servicio futuras o previstas se describen normalmente con una arquitectura objetivo. Se cubren así los bloques constituyentes, tales como las aplicaciones

futuras y el modelo de infraestructura objetivo, describiéndose asimismo los nexos y relaciones entre dichos bloques constituyentes.
- Las **buenas prácticas** para las capacidades de servicio incluyen:
  – La definición de los principios de la arquitectura (guías generales que gobiernan la implementación y el uso de recursos relacionados con TI dentro de la empresa)
  – La definición de las perspectivas arquitectónicas más adecuadas (para satisfacer las necesidades de las distintas partes interesadas)
  – Un repositorio de arquitecturas (el cual se puede utilizar para almacenar distintos tipos de resultados arquitectónicos) y niveles de servicio que deben ser definidos y conseguidos por los proveedores del servicio

Existen buenas prácticas externas para entornos de arquitectura y capacidades de servicio. Se trata de guías, modelos o estándares que pueden usarse para acelerar la creación de entregables de arquitectura.

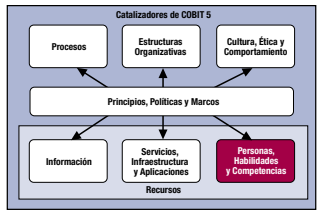
7.2 Servicios, Infraestructuras y Aplicaciones de Seguridad de la Información

Se precisa de capacidades de servicio que proporcionen a la empresa seguridad de la información y funcionalidades relacionadas. Los servicios no solo requieren infraestructuras y aplicaciones, sino que se ofrecen mediante una combinación de otros catalizadores tales como los procesos, la información y las estructuras organizativas.

La siguiente lista contiene algunos ejemplos de servicios potencialmente relacionados con la seguridad tal y como podrían aparecer en un catálogo de servicios. Normalmente, estos servicios están vinculados a uno o más procesos de COBIT 5 y a sus prácticas y actividades, y requieren información (entradas y salidas) y estructuras organizativas (matrices RACI, roles o funciones de seguridad específicos). La siguiente lista proporciona una visión orientada al servicio de las actividades relacionadas con la seguridad y no pretende duplicar o replicar procesos de seguridad:
- Proporcionar una arquitectura de seguridad.
- Proporcionar concienciación sobre seguridad.
- Proporcionar un desarrollo seguro (desarrollo alineado con los estándares de seguridad).
- Proporcionar evaluaciones de seguridad.
- Proporcionar sistemas adecuadamente securizados y configurados, en línea con los requerimientos de seguridad y la arquitectura de seguridad.
- Proporcionar acceso a los usuarios y derechos de acceso de acuerdo con los requerimientos del negocio.
- Proporcionar una adecuada protección frente al software malicioso, ataques externos e intentos de intrusión.
- Proporcionar una adecuada respuesta frente a incidentes.
- Proporcionar pruebas de seguridad.
- Proporcionar servicios de monitorización y alerta para eventos relacionados con la seguridad.

Para cada una de estas capacidades de servicio, los bloques de servicios constituyentes se han descrito en el **apéndice F**:
- Una **descripción detallada** del servicio, proporcionando funcionalidad al negocio
- **Atributos**, describiendo para cada servicio las entradas y tecnologías de apoyo (incluyendo aplicaciones e infraestructura)
- **Metas**, describiendo los objetivos de calidad y cumplimiento para cada capacidad de servicio y las métricas relacionadas

Capítulo 8
Catalizador: Personas, Habilidades y Competencias

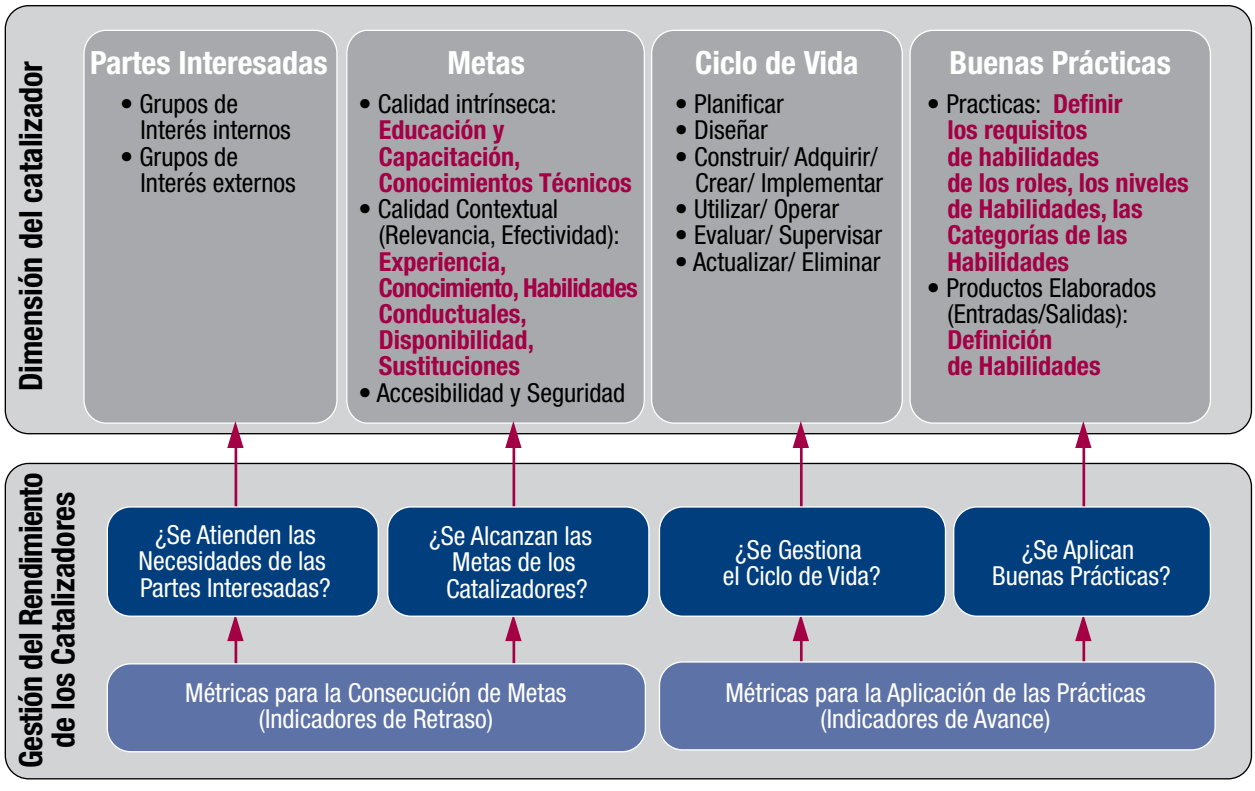


Las personas deben demostrar las habilidades y competencias adecuadas para asegurar que todas las actividades se completan con éxito y que se toman las decisiones correctas.
En este capítulo se revisan los siguientes elementos:
1. El modelo de habilidades y competencias
2. Habilidades y competencias relacionadas con la seguridad de la información

8.1 Modelo de Personas, Habilidades y Competencias

El personal, las habilidades y las competencias se pueden estructurar conforme a las dimensiones ilustradas en el modelo de catalizador de la **figura 19**.

Figura 19—Catalizador COBIT 5: Personas, habilidades y Competencias



La **figura 19** muestra los diferentes componentes del personal, habilidades y competencias tal y como están definidos en esta publicación. Este modelo de proceso es una extensión del modelo genérico de catalizadores explicado en la **figura 8**.

El modelo de personal, habilidades y competencias indica que:
- Diferentes **partes interesadas** pueden asumir diferentes roles (p.ej. gerente de negocio, jefe de proyecto, socio, competidor, reclutador, formador, desarrollador, especialista técnico de TI, ISM, CISO, regulador), y cada rol requiere un conjunto de habilidades distinto.
- Los **objetivos para las habilidades y las competencias** están vinculados a grados de educación y cualificación, habilidades técnicas, niveles de experiencia, conocimiento, y destrezas conductuales necesarias para proporcionar e implementar satisfactoriamente actividades de proceso, roles de la organización, etc. Las **metas para los recursos humanos** incluyen niveles adecuados de disponibilidad del personal y ratios de rotación.
- Las habilidades y competencias tienen un **ciclo de vida**. Una compañía debe conocer su línea base de habilidades actual y planificar de acuerdo con lo que debe ser. En ello influyen, entre otros factores, la estrategia y metas de la empresa. Las habilidades deben ser desarrolladas (p.ej. mediante formación), adquiridas (p.ej. mediante contratación) y desplegadas en los diversos roles dentro de la estructura de la organización, y pueden incluso descartarse (p.ej. si

una actividad se automatiza o externaliza). La empresa debe, periódicamente, evaluar su línea base de habilidades para comprender la evolución que ha tenido lugar.
- Las **buenas prácticas** sobre destrezas y competencias incluyen la definición de la necesidad de requisitos objetivos para las habilidades y para cada rol asumido por las diversas partes interesadas. Esto puede describirse mediante diferentes niveles de habilidades en diferentes categorías, para cada una de las cuales debería estar disponible una definición de cada habilidad. Las categorías de las habilidades corresponden a las actividades relacionadas con TI acometidas; en este caso, funciones relacionadas con la seguridad de la información.

Este capítulo describe las habilidades y aptitudes al nivel óptimo posible. En la realidad, sin embargo, las empresas pueden no siempre requerir este nivel óptimo de habilidades, o pueden no ser capaces de emplear recursos que demuestren un nivel óptimo de destrezas.

8.2 Habllidades y Competencias Relacionadas con la Seguridad de la Información

Para implementar con eficiencia una función de seguridad de la información dentro de una empresa, deben ejercer esta función los individuos con un conocimiento y experiencia (p.ej., destrezas y aptitudes) apropiados.

En la **figura 20** se listan algunas habilidades y aptitudes típicas relacionadas con la seguridad. Mientras en empresas más grandes estas habilidades se pueden traducir en puestos específicos (p.ej., las habilidades en arquitectura de seguridad de la información pueden equivaler a un puesto para un arquitecto de seguridad de la información) este puede no ser el caso en empresas más pequeñas.

Figura 20—Habilidades/Competencias de Seguridad de la Información

Habilidades/Competencias
Gobierno de seguridad de la información
Formulación estratégica de seguridad de la información
Gestión del riesgo de la información
Desarrollo de la arquitectura de seguridad de la información
Operaciones de seguridad de la información
Evaluación, pruebas y cumplimiento de la información

Para cada una de las habilidades y aptitudes de la **figura 20**, se describen los siguientes atributos en el **apéndice G**:
- **Definición de la habilidad**
- **Objetivos**—Según se han definido anteriormente
- **Catalizadores relacionados**—Se requieren habilidades y competencias para llevar a cabo actividades de proceso y para tomar decisiones en las estructuras organizativas. A su vez, algunos procesos están orientados a dar soporte al ciclo de vida de destrezas y competencias.

El valor añadido de la certificación en seguridad de la información:
Los atributos de las habilidades y competencias se alinean con los análisis de las prácticas de las certificaciones de ISACA: Certificado de Auditor de Sistemas de Información CISA), Certificado de Gestor de Seguridad de la Información (CISM), Certificado en el Gobierno de TI en Empresas (CGEIT), Certificado en el Control del Riesgo y de los Sistemas de Información (CRISC), y Profesional certificado en seguridad de sistemas (CISSP) del (ISC)[2]. Dado que la certificación es un medio objetivo para demostrar a los empleadores que los profesionales tienen un conocimiento de base dentro de un dominio, una certificación CISM o equivalente se sugiere para todas las habilidades definidas anteriormente.

Las habilidades y competencias siguen un ciclo de vida. Una actividad de seguridad de la información debe identificar su línea base de habilidades actual, y alinear esa línea base con el conjunto de habilidades requerido. En ello influyen (entre otros aspectos) la estrategia y objetivos de seguridad de la información. Las habilidades han de ser desarrolladas (p.ej. mediante formación presencial e interactiva) o adquiridas (p.ej. mediante contratación) y desplegadas en los distintos roles dentro de la estructura. Las habilidades pueden necesitar ser realineadas si, por ejemplo, una actividad se automatiza o externaliza. Periódicamente, por ejemplo, anualmente, la empresa precisa evaluar su línea base de habilidades para comprender la evolución que ha tenido lugar; esta evaluación alimentará el proceso de planificación del período siguiente. La evaluación también puede alimentar el proceso de reconocimiento y recompensa de las personas.

Nótese que los atributos que describen las habilidades y competencias son un conjunto de criterios y no una descripción obligatoria de un puesto. Las decisiones sobre contratación deberían ser tomadas en función de todos los factores previamente descritos así como la adecuación general del individuo a la empresa.

Sección III. Adaptando *COBIT 5 para Seguridad de la Información* al Entorno de la Empresa

Capítulo 1
Introducción

La seguridad de la información es valorable en una empresa solamente cuando está suficientemente adaptada a la situación única en la que esa empresa existe y opera. Esta situación única se crea por numerosos elementos de desafío asociados al cambio del entorno. La Sección II describe los catalizadores específicos de seguridad de la información que pueden utilizarse para la mejora de la madurez/capacidad/rendimiento de la seguridad de la información en la empresa. Adaptar estos catalizadores específicos al entorno empresarial es el desafío que se describirá en esta sección.

ISACA proporciona una guía de implementación completa y práctica concerniente al gobierno de las TI corporativas en su publicación *COBIT® 5 Implementación*,[4] que se basa en un ciclo de mejora continua. Esta guía no pretende ser un enfoque prescriptivo, sino más bien una guía para profesionales de la seguridad de la información que necesitan integrar la seguridad dentro del marco operacional completo de una empresa. La guía también se apoya en un kit de herramientas de implementación que contiene varios recursos que serán mejorados continuamente. Su contenido incluye:
- Herramientas de autoevaluación, medición y diagnóstico.
- Presentaciones orientadas a diferentes audiencias.
- Artículos relacionados y explicaciones adicionales.

El propósito de esta sección es introducir el ciclo de implementación y mejora continua hasta alcanzar un alto nivel y describe esta guía genérica desde la perspectiva de la seguridad de la información. Además, la relación con los marcos de trabajo de la seguridad de la información, las buenas prácticas y estándares existentes se describe en la segunda parte de esta sección.

[4] ISACA, *COBIT 5 Implementación*, EE.UU., 2012, *www.isaca.org/cobit*

Página dejada en blanco intencionadamente

Capítulo 2
Implementación de Iniciativas de Seguridad de la Información

2.1 Considerando el Contexto Empresarial de la Seguridad de la Información

Cada empresa necesita definir e implementar sus propios catalizadores de la seguridad de la información dependiendo de los factores específicos de los entornos internos y externos de la empresa, tales como:
- Ética y cultura relativas a la seguridad de la información
- Leyes, regulaciones y políticas aplicables
- Regulaciones contractuales aplicables
- Políticas y prácticas existentes
- Nivel de madurez de los catalizadores de la seguridad de la información actuales
- Las capacidades de la seguridad de la información y recursos disponibles
- Prácticas de la industria
- Estándares obligatorios y marcos de trabajo existentes con respecto de la seguridad de la información

Los requerimientos de la seguridad de la información de la empresa necesitan definirse basándose en:
- Planes e intenciones estratégicas del negocio
- Estilo de gestión
- Perfil de riesgo de la información
- Apetito de riesgo

Por consiguiente, el alcance para la implementación de las iniciativas de la seguridad de la información será diferente para cada empresa y es necesario comprender y considerar el contexto para adaptar eficazmente *COBIT 5 para Seguridad de la Información.* Es igualmente importante aprovechar y construir sobre los catalizadores específicos para la seguridad de la información existentes.

> COBIT 5 para Seguridad de la información **conecta con otros marcos de trabajo, buenas prácticas y estándares:** *COBIT 5 para Seguridad de la información* iestá respaldado por otros marcos de trabajo, buenas prácticas y estándares. Estos deberían proporcionar detalles a los profesionales de la seguridad de la información sobre temas específicos para optimizar los catalizadores descritos en esta publicación. La conexión de *COBIT 5 para Seguridad de la Información* apuntala estos marcos de trabajo, buenas prácticas y estándares que se describen en la siguiente parte de esta sección.

En general, los factores clave de éxito para una implementación con éxito de los catalizadores de la seguridad de la información incluyen:
- La dirección y mandato para la iniciativa de la seguridad de la información, así como el compromiso y apoyo visible y continuo de la alta dirección
- La iniciativa de la seguridad de la información entiende el negocio y los objetivos de TI apoyados por todas las partes
- Comunicación eficaz y habilitación de los necesarios cambios garantizados
- *COBIT 5 para Seguridad de la Información* y otros apoyos de buenas prácticas y estándares adaptados para encajar en el contexto único de la empresa
- Centrarse en resultados rápidos y priorizando las mejoras más fáciles de implementar.
- Adecuada financiación y compromiso de recursos
- Recursos humanos adecuadamente preparados que puedan implementar los catalizadores

2.2 Creando el Entorno Apropiado

Para que las iniciativas de la seguridad de la información se aprovechen de COBIT es importante que estén adecuadamente gobernadas y gestionadas. Las principales iniciativas relacionadas con TI a menudo fracasan debido a una dirección, respaldo y vigilancia inadecuados de las partes interesadas; la implementación de los catalizadores de seguridad de la información utilizando esta publicación no es diferente. El apoyo y la dirección de las partes interesadas más importantes son críticos para garantizar que se consiguen y mantienen las mejoras. En un entorno de empresa débil (así como en el de una estrategia general de la seguridad de la información poco clara), este apoyo y participación es incluso más importante.

El uso de catalizadores (aprovechando *COBIT 5 para Seguridad de la Información*) debería ser una solución real para las necesidades y cuestiones del negocio más allá de un fin en sí mismo. Los requerimientos de la seguridad de la información basados en los puntos débiles y elementos clave actuales deberían ser identificados y aceptados por la dirección como áreas que necesitan ser consideradas. Los chequeos de salud de alto nivel, diagnósticos o evaluaciones de capacidad basados en esta publicación son herramientas que pueden utilizarse para tomar conciencia, crear consenso y generar un

compromiso para actuar. El compromiso y la adhesión de las partes interesadas más importantes se debe solicitar desde el comienzo. Para conseguirlo, los objetivos y beneficios de la implementación deben estar claramente expresados en los términos del negocio y resumidos en un esbozo de caso de negocio.

Una vez obtenido el compromiso, es necesario contar con los recursos adecuados para apoyar el programa de la seguridad de la información. Se deben definir y asignar los roles y responsabilidades clave. Se debería cuidar el mantenimiento de forma permanente del compromiso de todas las partes interesadas afectadas.

Para dirigir y vigilar se deben establecer y mantener estructuras y procesos adecuados. Estas estructuras y procesos también deben garantizar el alineamiento continuo con la gobernanza de toda la empresa, el enfoque de la gestión de riesgos y la estrategia del negocio.

Las partes interesadas clave, así como los ejecutivos sénior, deben proporcionar apoyo y compromiso visibles para establecer "el tono en la cúspide" y asegurar el compromiso de todos los niveles en el programa de la seguridad de la información.

2.3 Reconociendo Puntos Débiles y Eventos Desencadenantes

Hay varios factores que pueden indicar una necesidad para mejorar los catalizadores de la seguridad de la información. Al utilizar puntos débiles o eventos desencadenantes como punto de lanzamiento para la implementación de iniciativas, el caso de negocio para la mejora del catalizador de la seguridad de la información puede estar relacionado con aspectos prácticos, diarios. Esto debería mejorar su aceptación y crear un sentido de urgencia dentro de la empresa, necesario para lanzar la implementación.

En resumen, se pueden identificar ganancias rápidas y se pueden demostrar valores añadidos en aquellas áreas que sean más visibles o reconocibles en la empresa. Esto proporciona una plataforma para introducir más cambios y puede ayudar en la obtención del compromiso y el apoyo amplio de la dirección sénior a cambios más generales.

Algunos ejemplos de típicos puntos débiles para los que unos nuevos o revisados catalizadores de la seguridad de la información pueden ser la solución son:
- Incidentes de seguridad de la información en la empresa o en los competidores tales como:
  - La pérdida o robo de información causada por usuarios no autorizados que irrumpen en el sistema
  - Denegación de servicio como resultado de ciberataques
  - Modificaciones (no)intencionadas de información crítica
- Fallos en el cumplimiento de requerimientos legal, regulatorio o contractuales, así como las reglas de privacidad
- La incapacidad de incorporar nueva tecnología debido a las restricciones de la seguridad de la información
- Hallazgos de auditoría regularmente relacionados con las pobres capacidades de la seguridad de la información.

Además de estos puntos débiles, otros eventos internos o externos del entorno de la empresa pueden ser señal o desencadenar la atención sobre el gobierno y la gestión de las TI corporativas. Ejemplos de esto incluye:
- Nuevos requisitos de regulación, cumplimiento o contractuales
- Cambios significativos de tecnología o cambios de paradigma
- Auditorías externas o evaluaciones de consultores
- Fusiones, adquisiciones u otros cambios organizativos mayores

2.4 Posibilitar el Cambio

El éxito de la implementación depende de la gestión del cambio de forma eficaz. En muchas empresas, hay un foco significativo sobre los aspectos técnicos del programa de seguridad de la información, pero no suficiente énfasis en la gestión de los aspectos humanos, de comportamiento y culturales del cambio y en la motivación a las partes interesadas para que se incorporen a ese cambio.

No se debería asumir que varías partes interesadas involucradas, o impactadas por, los catalizadores de la seguridad de la información nuevos o revisados aceptarán y adoptarán rápidamente los cambios propuestos. La posibilidad de ignorancia y/o la resistencia al cambio necesita abordarse mediante un enfoque estructurado y proactivo. En apoyo de esto, se logrará una óptima toma de conciencia del programa de implementación mediante un plan de comunicación que defina para cada fase del programa que será comunicado, de qué forma y por quién.

Se puede lograr una mejora sostenible obteniendo el compromiso de las partes interesadas mediante persuasión y recomendación o, donde sea posible, obligación de cumplimiento de la legislación, regulaciones o acuerdos contractuales. En otras palabras, se han de tener en cuenta cuestiones humanas, costumbres y de cultura para crear una cultura en la que las partes interesadas sean participantes activos en alcanzar los objetivos de seguridad de la empresa.

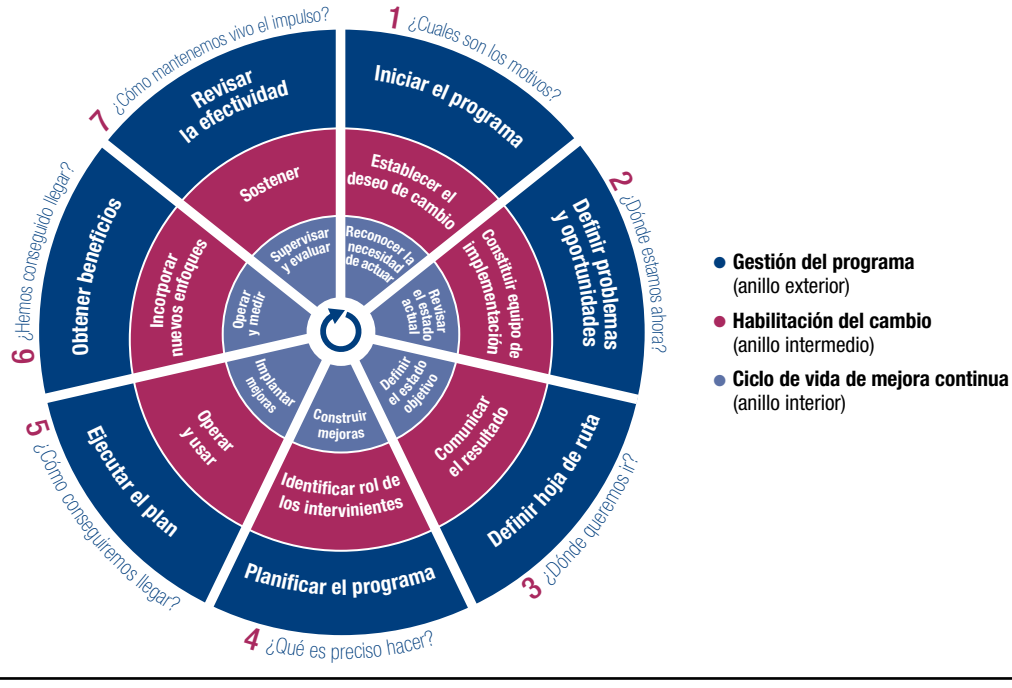
Cultura de seguridad de la información y cambio:
Las prácticas de los catalizadores de la cultura, éticas y costumbres que se presentan en esta sección II son, de lejos, las herramientas más importantes para reducir cualquier resistencia al cambio. La influencia en los comportamiento mediante una comunicación eficaz, una identificación de los incentivos y recompensaciones correctas y relevantes, y forzar la adherencia a los cambios son importantes factores a tener en cuenta. Invertir en prácticas de influencia posibilitará la aceptación de los cambios realizados. Por supuesto esto requerirá tiempo y paciencia de los miembros del equipo de la seguridad de la información.

2.5 Un Enfoque del Ciclo de Vida

La implementación del ciclo de vida proporciona a las empresas una manera de solucionar la complejidad y los desafíos que normalmente aparecen durante las implementaciones usando COBIT para contemplar la seguridad de la información. Hay tres componentes interrelacionados del ciclo de vida (ver los círculos de la **figura 21**):
• El ciclo de vida de mejora continua –Lo que refleja que esto no es un proyecto puntual
• La habilitación del cambio – Abordar los aspectos de comportamiento y culturales
• La gestión del programa

Como se ha comentado anteriormente, se debe crear el entorno apropiado para asegurar el éxito de la implementación o de la iniciativa de mejora. El ciclo de vida y sus siete fases se ilustran en la **figura 21**.

Figura 21—Las Siete Fases de la Implementación del Ciclo de Vida



El propósito de la **fase 1** es comprender la amplitud y profundidad de los cambios previstos, las diversas partes interesadas que están afectadas, la naturaleza del impacto y la participación de cada grupo de partes interesadas, así como la preparación y capacidad de adaptarse al cambio.

El entorno de la seguridad de la información:
Los puntos débiles y eventos desencadenantes relativos a seguridad de la información deberían evaluarse a fondo. Las prácticas operativas presentadas en el catalizar información en la sección II pueden ser muy útiles para esta evaluación. Los informes de revisión de la seguridad de la información, incluyendo resultados de auditoría e informes de riesgo o el cuadro de mando de la seguridad de la información pueden proporcionar una entrada importante sobre incidentes de seguridad, problemas y riesgos. Las discusiones con la dirección ejecutiva deberían proveer una plataforma para establecer el deseo de cambio presentando temas e informes de una manera clara y comprensible.

La **Fase 2** está enfocada en definir el alcance de la iniciativa de implementación o mejora. Un diagnóstico a alto-nivel puede ser de utilidad para determinar el alcance y conocer las áreas de mayor prioridad en las cuales enfocarse. Se realiza entonces una evaluación del estado actual de cada fase, y se identifican cuestiones o deficiencias a través de una evaluación de capacidades de procesos. Las iniciativas de gran escala deben ser estructuradas como interacciones

múltiples del ciclo de vida. Para cualquier iniciativa de implantación que exceda los 6 meses, existirá un riesgo de perder el impulso, el foco y la aceptación de los grupos de interés.

Determinación del alcance de la seguridad de la información:
Para determinar el alcance de la iniciativa de la seguridad de la información, el estado actual de todos los catalizadores de la seguridad de la información debería ser evaluado y verificado. Para los procesos, la determinación del alcance puede estar basada en los objetivos de la seguridad de la información asociados a procesos de TI (como se documenta en la sección II de la guía detallada de procesos). Sería útil considerar como los escenarios de riesgo pueden resaltar procesos clave en los cuales enfocarse.

Durante la **Fase 3**, se fija un objetivo de mejora, acompañado de un análisis más detallado utilizando esta publicación y otras guías (ver sección III, 2.2 Creando el Entorno Apropiado) para identificar desajustes y posibles soluciones. Algunas soluciones pueden ser ganancias rápidas y otras, actividades más retadores y a más largo plazo. La prioridad debe ser dada a las iniciativas que sean más sencillas de conseguir y aquellas que probablemente rindan los mayores beneficios.

Usando la dirección de la seguridad de la información:
En la siguiente parte de esta sección, se proporciona orientación adicional para conectar marcos de seguridad de la información, buenas prácticas y estándares usados comúnmente. Una fase importante en el ciclo de vida de la implantación es la fijación correcta de objetivos y determinar cómo los marcos de trabajo para la seguridad de la información, buenas prácticas y estándares relevantes pueden ayudar a la empresa en la consecución de este objetivo.

Las ganancias rápidas (iniciativas con alto impacto y bajo esfuerzo) para una iniciativa de la seguridad de la información son a menudo muy desafiantes. El hecho del constante equilibrio entre asegurar la seguridad de la información y posibilitar a la empresa debe siempre ser tenido en cuenta cuando se definan estas ganancias rápidas. Los cambios visibles son necesarios para que una ganancia rápida demuestre rápidamente el valor añadido a la empresa.

La **Fase 4** planea soluciones prácticas definiendo proyectos apoyados por casos de negocio justificables. También se desarrolla un plan de cambio para la implantación. Un caso de negocio bien desarrollado ayuda a asegurar que los beneficios del proyecto son identificados y controlados. Se pueden definir y supervisar medidas usando los objetivos y métricas de *COBIT 5 Seguridad de la Información* para asegurar que la alineación con el negocio está garantizada y mantenida y el rendimiento pueden ser medido.

La **Fase 5** implementa las soluciones propuestas en prácticas del día a día. Para tener éxito, es necesario el compromiso y la demostrada implicación del equipo de alta dirección, así como la toma de propiedad por las partes afectadas del negocio y las partes interesadas de TI.

La **Fase 6** se focaliza en la sostenibilidad de las operaciones de los nuevos o mejorados catalizadores y la supervisión de la consecución de los beneficios esperados. En otras palabras, esta fase sirve para determinar si los objetivos se han alcanzado y son sostenibles.

Durante la **Fase 7**, se revisa el éxito en conjunto de la iniciativa, se identifican requerimientos adicionales para la seguridad de la información de la empresa, y se refuerza la necesidad de mejora continua. Con el tiempo, el ciclo de vida debe ser seguido de forma iterativa mientras se construye un acercamiento sostenible a la seguridad de la información.

Capítulo 3
Usando *COBIT 5 para Seguridad de la Información* para Conectar Otros Marcos de Trabajo, Modelos, Buenas Prácticas y Estándares

COBIT 5 para Seguridad de la Información pretende ser un marco de trabajo "paraguas" para conectar con otros marcos de trabajo, buenas prácticas y estándares de seguridad de la información. *COBIT 5 para Seguridad de la Información* describe la omnipresencia de la seguridad de la información a lo largo de toda la empresa y provee un marco genérico de catalizadores, pero otras publicaciones pueden ser de ayuda también porque desarrollan aspectos más concretos (p. ej. prácticas para la seguridad de la información o guías de configuración). Los marcos, buenas prácticas y estándares relevantes para seguridad de la información necesitan ser adaptados para encajar en requerimientos específicos del entorno específico de la empresa. El lector puede entonces decidir, sobre la base de las necesidades específicas de la empresa, qué marco o combinación de marcos es mejor utilizar, teniendo también en consideración la situación heredada, la disponibilidad del marco y otros factores. Para esto, el mapa de COBIT 5 Seguridad de la Información con los estándares relacionados del **apéndice H** ayudará a encontrar un marco adecuado según las necesidades relevantes.

Ejemplos de marcos y modelos, buenas prácticas y estándares relevantes para la seguridad de la información son:
- *Business Model for Information Security* (BMIS), ISACA, EE.UU., 2010
- *2011 Standard of Good Practice for Information Security, Information Security Forum (ISF),* Reino Unido, 2011
- *Common Security Framework (CSF), Health Information Trust Alliance (HITRUST),* EE.UU., 2009
- *Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS), Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI),* Ministerio de Defensa, Francia, 2000
- *Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH),* EE.UU., 1996 y 2009, respectivamente
- *Series ISO/IEC 2700,* Suiza, 2009-2012
- *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53A, Guide for Assessing the Information Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans,* Departamento de Comercio, EE.UU., 2010
- *Operational Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE®), Carnegie Mellon Software Engineering Institute (SEI),* EE.UU., 2001
- *Payment Card Industry Data Security Standards (PCI DSS) v2.0, PCI Security Standards Council,* EE.UU., 2010

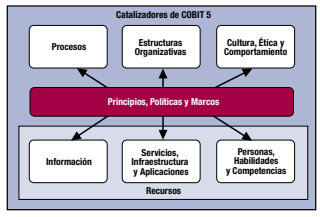
Además, una vez se ha identificado la guía más adecuada, *COBIT 5 para Seguridad de la Información* puede ser usado para estructurar los contenidos de estas publicaciones y realizar un análisis de diferencias, como se describe en la fase 3 de del ciclo de vida de la implantación.

Sin embargo, es importante hacer notar que los estándares relacionados con la seguridad de la información y sus áreas relacionadas son abundantes y están en constante evolución; por lo tanto este capítulo refleja muchos de los estándares disponibles.

En el **apéndice H** presenta una detallada plantilla para comparar y evaluar las siguientes publicaciones:
- *The 2011 Standard of Good Practice for Information Security, Information Security Forum (ISF)*, Reino Unido, 2011, *www.securityforum.org/?page=publicdownload2011sogp*
- *ISO/IEC 27001 y 27002,* Suiza, 2005, *www.iso.org/iso/store.htm*
- NIST SP 800-53A, *Guide for Assessing the Information Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, Departamento de Comercio, EE.UU., 2010, *http://csrc.nist.gov/publications/PubsSPs.html*

Página dejada en blanco intencionadamente

Apéndice A
Guia Detallada: Catalizador de Principios, Políticas y Marcos



Este apéndice provee detalles acerca de los principios y políticas para la seguridad de la información presentadas en la sección II. Los principios para la seguridad de la información comunican las reglas de la empresa para apoyar los objetivos de gobierno y los valores empresariales, como hayan sido definidos por el Consejo y el comité ejecutivo de dirección. Estos principios son desarrollados en detalle en la subsección A.1 de este apéndice.

Adicionalmente, las políticas proporcionan una guía más detallada sobre cómo aplicar los principios a la práctica y cómo influirán en la toma de decisiones. Los ejemplos de políticas incluyen:
- Política de seguridad de la información
- Política de control de accesos
- Política de seguridad de la información del personal
- Política de seguridad física y ambiental
- Política de gestión de incidentes
- Política de continuidad de negocio y recuperación ante desastres
- Política de gestión de activos
- Reglas de comportamiento (uso aceptable)
- Política de adquisición, desarrollo de software y mantenimiento de sistemas informáticos
- Política de gestión de proveedores
- Política de gestión de comunicaciones y operaciones
- Política de cumplimiento
- Política de gestión de riesgos

Para cada una de las políticas presentadas en la sección II, los siguientes atributos se describen en este apéndice:
- **Alcance**
- **Validez** (excepto para las políticas de seguridad de la información dirigidas por otras funciones dentro de la organización)
  - **Aplicabilidad**—¿A qué áreas de la organización se aplica esta política?
  - **Actualización y revalidación**—¿Quién es el responsable de mantener la política y cuál es la frecuencia de revalidación?
  - **Distribución**—¿Cómo se deberían distribuir las políticas en la empresa?
- **Metas** (excepto para las políticas para la seguridad de la información dirigidas por otras funciones dentro de la empresa)

A.1 Principios de la Seguridad de la Información

En 2010, tres organizaciones globales líderes en seguridad de la información – ISACA, ISF e (ISC)²—unieron fuerzas para desarrollar 12 principios independientes y no propietarios que ayudarán a los profesionales de la seguridad de la información a añadir valor a sus organizaciones mediante un apoyo al negocio con éxito y la promoción las de buenas prácticas para la seguridad de la información (*www.isaca.org/Knowledge-Center/Standards/Pages/Security-Principles.aspx*). Estos principios están estructurados para dar soporte a tres tareas:
- Dar soporte al negocio.
- Defender el negocio.
- Promover un comportamiento responsable en seguridad de la información.

Estos tres principios, en la **figura 22**, son genéricos y aplicables a todas las compañías. Esta lista puede ser usada como base para el desarrollo de principios para la seguridad de la información únicos para la empresa.

Figura 22—Principios para la Seguridad de la Información

Principio	Objetivo	Descripción
1. Dar soporte al negocio.		
Entregar calidad y valor a las partes interesadas.	Asegurar que la seguridad de la información entrega valor y cumple los requerimientos de negocio.	Las partes interesadas internas y externas deben estar comprometidas a través de comunicaciones regulares de forma que sus requerimientos cambiantes puedan continuar siendo alcanzables. La promoción del valor de la seguridad de la información (tanto financiero como no-financiero) ayuda a ganar apoyo para la toma de decisiones, las cuales pueden convertirse en ayuda para el éxito de la visión de la seguridad de la información.

Figura 22—Principios para la Seguridad de la Información *(cont.)*		
Principio	**Objetivo**	**Descripción**
1. Apoyo al negocio. ***(cont.)***		
Cumplir con los requerimientos legales y regulatorios relevantes.	Asegurar que se cumplen las obligaciones estatuarias, se gestionan las expectativas de las partes interesadas, y se evitan las sanciones criminales o civiles.	Las obligaciones de cumplimento deben ser identificadas, traducidas a requerimientos específicos para la seguridad de la información y comunicadas a todas las personas relevantes. Las sanciones asociadas al no-cumplimiento deben ser claramente entendidas. Los controles deben supervisados, analizados y mantenidos al día para cumplir con nuevos o actualizados requisitos legales o regulatorios.
Proveer información oportuna y exacta sobre el rendimiento de la seguridad de la información.	Apoyar los requerimientos del negocio y gestionar los riesgos de la información.	Los requerimientos para proveer información sobre el rendimiento de la seguridad de la información deben estar claramente definidos, apoyados por las más relevantes y exactas métricas de seguridad de la información (como cumplimiento, incidentes, controles de estado y costes) y alineadas con los objetivos de negocio. La información debe ser capturada de forma periódica, consistente y rigurosa, de manera que sea información correcta y los resultados puedan presentarse para satisfacer los objetivos de las partes interesadas relevantes.
Evaluar las amenazas actuales y futuras de la información.	Analizar y evaluar las amenazas emergentes en seguridad de la información de forma que se puedan tomar acciones a tiempo y con información para mitigar el riesgo.	Se deben clasificar en un marco de trabajo exhaustivo y estándar las grandes tendencias y las amenazas específicas de la seguridad de la información, cubriendo un amplio rango de temas, tales como aspectos políticos, legales, económicos, socio culturales y técnicos. Las personas deben compartir y adquirir conocimiento sobre nuevas amenazas para considerar proactivamente sus causas, más que sus síntomas.
Promover la mejora continua en la seguridad de la información.	Reducir costes, mejorar la eficacia y eficiencia, y promover una cultura de mejora continua en la seguridad de la información.	Los constantemente cambiantes modelos de negocio -emparejados con las amenazas en evolución- requieren que las técnicas para la seguridad de la información se deaen adaptar y mejorar su nivel de eficacia de forma continua. Deben conocerse las últimas técnicas de seguridad de la información aprendiendo de los incidentes y estando en contacto con organismos de investigación independientes.
2. Defender el negocio.		
Adoptar un enfoque basado en el riesgo.	Asegurar que el riesgo se trata de forma consistente y eficaz.	Las opciones para abordar riesgos de la información deben ser revisadas de forma que se tomen decisiones informadas y documentadas sobre el tratamiento del riesgo. El tratamiento de los riesgos implica elegir entre una o más opciones, las cuales normalmente incluyen: • Aceptar el riesgo (mediante un miembro directivo que firma que él/ella ha aceptado el riesgo y no es necesario realizar acciones adicionales) • Evitar el riesgo (p. ej., decidiendo no perseguir una iniciativa particular) • Transferir el riesgo (p. ej., externalizando o contratando un seguro) • Mitigar el riesgo(normalmente aplicando las medidas apropiadas de seguridad de la información, p. ej., controles de acceso, controles de red y gestión de incidentes)
Proteger la información.	Prevenir la revelación de información clasificada (p. ej. confidencial o sensible) a individuos no autorizados.	La información debe ser identificada y después clasificada de acuerdo a su nivel de confidencialidad (p. ej. secreta, restringida, interna y publica). La información clasificada debe ser protegida apropiadamente a lo largo de los estados de su ciclo de vida -desde su creación a su destrucción- usando los controles apropiados como cifrado o restricción de accesos.
Centrarse en las aplicaciones de negocio críticas.	Priorizar los escasos recursos de la seguridad de la información protegiendo las aplicaciones de negocio en las cuales un incidente en la seguridad de la información tendría el mayor impacto en el negocio.	Entender el impacto en el negocio de una pérdida de integridad o disponibilidad de información importante manejada por las aplicaciones de negocio (procesada, almacenada o transmitida) ayudará a establecer el nivel de criticidad. Los requisitos de recursos para la seguridad de la información pueden ser entonces determinados y emplazados con prioridad en proteger las aplicaciones que son más críticas para el éxito de la empresa.
Desarrollar sistemas de forma segura.	Construir sistemas de calidad y de manera eficaz en los cuales el personal delnegocio pueda confiar (p. ej. que sean consistentemente robustos, exactos y confiables).	La seguridad de la información debe estar integrada en las fases de definición del alcance, diseño, construcción y pruebas del ciclo de vida de desarrollo (SDLC). Las buenas prácticas para la seguridad de la información (p. ej. pruebas rigurosas para detectar debilidades de la seguridad de la información; revisión por iguales; y la habilidad de hacer frente a errores, excepciones y condiciones de emergencia) deben jugar un papel clave en todas las fases del proceso de desarrollo.

Figura 22—Principios para la Seguridad de la Información *(cont.)*		
Principio	**Objetivo**	**Descripción**
3. Promover un comportamiento responsable en seguridad de la información.		
Actuar de una manera profesional y ética.	Asegurar que las actividades relacionadas con la seguridad de la información se llevan a cabo de una manera fiable, responsable y eficaz.	La seguridad de la información depende en gran medida de la capacidad de los profesionales del sector para realizar sus funciones con responsabilidad y con plena consciencia de cómo su integridad tiene un impacto directo sobre la información que se encargan de proteger. Los profesionales de la seguridad de la información necesitan estar comprometidos con un alto nivel de calidad en su trabajo, al tiempo que demuestran un comportamiento coherente y ético, y respeto hacia las necesidades del negocio, hacia otros individuos y hacia la información (a menudo personal) confidencial.
Fomentar una cultura positiva de la seguridad de la información.	Proporcionar una influencia positiva en el comportamiento de los usuarios finales respecto a la seguridad de la información, reducir la probabilidad de que se produzcan incidentes de seguridad de la información y limitar su impacto potencial en el negocio.	Se debe poner especial énfasis en hacer de la seguridad de la información una parte clave del día a día del negocio, aumentando la conciencia entre los usuarios y garantizando que éstos cuenten con las habilidades necesarias para proteger la información y los sistemas críticos o clasificados. Debe hacerse que los individuos tomen conciencia de los riesgos de la información a su cuidado y debe potenciárseles para que tomen las medidas necesarias para protegerla.

A.2 Política de Seguridad de la Información

Esta sección cubre la política de seguridad de información a alto nivel, describiendo el alcance de la política y de las personas involucradas. La información contenida en esta sección debería adaptarse a conveniencia de las necesidades específicas de una empresa.

Alcance

El aspecto y la extensión de una política de seguridad de la información varían ampliamente de unas empresas a otras. Algunas consideran que un resumen de una página es suficiente como política de seguridad de la información. En este caso, la política podría considerarse como una declaración de alto nivel y debe describir claramente los enlaces a otras políticas específicas. En otras empresas, la política de seguridad de la información está completamente desarrollada, conteniendo, casi en su totalidad, el nivel de detalle necesario para poner los principios en práctica. Es importante entender qué esperan las partes interesadas en la información, en términos de cobertura, y adaptarse a estas expectativas. La información contenida en el apéndice E, relativo al facilitador información, deberá resultar útil a este respecto.

Independientemente de su extensión o grado de detalle, la política de seguridad de la información necesita un alcance claramente definido. Esto incluye:

- Una definición de seguridad de la información para la empresa
- Las responsabilidades asociadas con la seguridad de la información
- La visión relativa a la seguridad de la información, acompañada de las metas y métricas apropiadas y una explicación de cómo dicha visión es apoyada por la cultura y la concienciación sobre seguridad de la información
- Explicación de cómo la política de seguridad de la información se alinea con otras políticas de alto nivel
- Elaboración de aspectos específicos de seguridad de información, tales como la gestión de datos, la evaluación de riesgos de la información y el cumplimiento de las obligaciones legales, reglamentarias y contractuales
- Potencialmente, la gestión del presupuesto y coste del ciclo de vida de la seguridad de información. Pueden añadirse, también, los planes estratégicos de seguridad de la información y la gestión de la cartera asociada a los mismos.

Esta lista no es exhaustiva; se pueden añadir más temas en el alcance dependiendo de la empresa. Es importante innovar constantemente y reutilizar buenas prácticas, las cuales pueden mejorarse a través de la comunicación, la presentación de informes y el gobierno necesario de la arquitectura y de la tecnología. También se deben tener en cuenta la organización específica y la interacción con las partes interesadas.

La política debería comunicarse activamente a toda la empresa y distribuirse a todos los empleados, contratistas, empleados temporales y terceros proveedores. Las partes interesadas deben conocer los principios de la información, los requisitos de alto nivel y los roles y responsabilidades para la seguridad de la información. La responsabilidad de actualizar y revalidar la política de seguridad de la información recae sobre la función de seguridad de la información (CISO/ISM).

A.3 Políticas Específicas de Seguridad de la Información Dirigidas por la Función de Seguridad de la Información

Esta subsección incluye varios ejemplos de políticas que son dirigidas por diferentes funciones de seguridad de la información. Las funciones consideradas incluyen el control de acceso, la información personal, la información física y

ambiental y los incidentes de seguridad. Para cada una de estas políticas, se ofrece una descripción que ilustra el alcance y las metas de la política y su distribución a la audiencia adecuada.

Política de Control de Acceso

La política de control de acceso proporciona un acceso adecuado a las partes interesadas, internas y externas, a fin de que se alcancen los objetivos del negocio. Esto se puede medir con métricas tales como el:
- El número de violaciones de acceso que exceden la cantidad permitida
- La cantidad de trabajo interrumpido debido a derechos de acceso insuficientes
- El número de incidentes o hallazgos de auditoría relativos a segregación de funciones

Adicionalmente, la política de control de acceso debería garantizar que el acceso de emergencia esté debidamente permitido y revocado en el momento oportuno. Las métricas relacionadas con este objetivo incluyen el:
- El número de solicitudes de acceso de emergencia
- El número de cuentas de emergencia activas que exceden los límites de tiempo aprobados

La política de control de acceso debería cubrir los siguientes temas, entre otros:
- El ciclo de vida del aprovisionamiento del acceso físico y lógico
- El criterio de menor privilegio o necesidad de conocer
- La segregación de funciones
- Acceso en caso de emergencia

Esta política está destinada a las correspondientes unidades de negocio, a los proveedores y a terceros. Las actualizaciones y revalidaciones deben involucrar a RRHH, a los propietarios de datos y sistemas y a seguridad de la información. Toda política nueva o actualizada debería distribuirse a las correspondientes unidades de negocio, a los proveedores y a terceros.

Política de Seguridad de la Información Relativa al Personal

El objetivo de la política de seguridad de la información relativa al personal incluye, entre otros, los siguientes objetivos:
- Realizar regularmente una verificación de antecedentes de todos los empleados y las personas en puestos clave. Este objetivo se puede medir a través del recuento del número de verificaciones de antecedentes completadas para el personal clave. Se puede ampliar con el número de renovaciones de verificaciones de antecedentes vencidas sobre la base de una frecuencia predeterminada.
- Obtener información sobre el personal clave en puestos de seguridad de información. Esto puede ser seguido por el recuento del número de personas en puestos clave que no han rotado de acuerdo con una frecuencia predefinida.
- Desarrollar un plan de sucesión para todos los puestos clave relacionados con la seguridad de información. Una posible medida es listar todos los puestos críticos de la seguridad de información que no cuentan con personal de respaldo.
- Verificar si todo el personal de seguridad de la información tiene las habilidades pertinentes y las certificaciones afines, vigentes. La escasez de personal adecuado o cualificado en los puestos críticos de seguridad de información podría reflejar el estado de este objetivo.

Esta política está destinada a las correspondientes unidades de negocio, a los proveedores y a terceros. Las actualizaciones y revalidaciones deben involucrar a RRHH, al director de privacidad, a asesoría jurídica, a seguridad de la información y al área de protección de instalaciones. Toda política nueva o actualizada deberá ser distribuida a los empleados, a los contratistas, a los proveedores según se especifique en contrato y a los empleados temporales.

Política de Seguridad Física y Ambiental

El objetivo de esta política es proporcionar orientación relativa a:
- Protección de ubicaciones físicas
- Controles ambientales que proporcionen capacidad a las operaciones de soporte.

La protección de la ubicación física puede ser medida a través del el número de vulnerabilidades explotables identificadas y/o por los incidentes atribuidos a las amenazas propias de la localización física (actos delictivos, riesgos industriales o de transporte, amenazas naturales). Los controles ambientales pueden ser verificados mediante la medición de la cantidad de vulnerabilidades explotables identificadas y/o incidentes atribuidos a los sistemas de control ambiental.

Indirectamente, la política contribuye a la optimización de los costes de los seguros. Una métrica relacionada puede ser la tendencia de los costes por seguros relacionados con la pérdida debido a las amenazas físicas, delictivas y medioambientales.

El alcance de la política puede incluir:
- Selección de instalaciones:
  – Criterios para la selección
  – Atributos de construcción

• Las normas de control medioambiental
• Las normas de control de acceso físico (para empleados, proveedores, visitantes)
• Supervisión de seguridad de la información y la detección de intrusiones físicas

Esta política está dirigida a los empleados, a todas las unidades de negocio, a los proveedores que porten activos/equipos de la organización y a todos los visitantes. Las actualizaciones y revalidación deberían involucrar al área de instalaciones, al de asesoría jurídica, a seguridad de la información y a los titulares de datos y sistemas. Toda política nueva o actualizada debería distribuirse a los empleados, a los contratistas, a los proveedores según se especifique en contrato y a los empleados temporales.

Política de Respuesta a Incidentes de Seguridad

El alcance de esta política cubre la necesidad de responder a los incidentes de una manera oportuna para recuperar las actividades de negocio. La política debería incluir:
• Una definición de incidente de seguridad de información
• Una declaración de cómo se manejarán los incidentes
• Requisitos para establecer el equipo de respuesta a incidentes, con roles y responsabilidades.
• Requisitos para la creación de un plan probado de respuesta a incidentes, que proporcionará los procedimientos y directrices documentados relativos a:
  – Criticidad de los incidentes
  – Procesos de comunicación (notificación) y escalado
  – Recuperación (incluidos):
    · Objetivos de Tiempo de Recuperación (RTOs) para volver al estado de confianza
    · Investigación y preservación del proceso
    · Pruebas y formación
  – Reuniones posteriores a los incidentes para documentar el análisis de las causas raíz, así como las mejoras en las prácticas de seguridad de la información para evitar futuros eventos similares.
• Documentación de los incidentes y cierre

Esta política está dirigida a las correspondientes unidades de negocio y a los empleados clave. Las actualizaciones y revalidación deberían involucrar a la función de seguridad de la información. Toda política nueva o actualizada debería distribuirse a los empleados clave.

A.4 Políticas Específicas de Seguridad de la Información Dirigidas por Otras Funciones Dentro de la Empresa

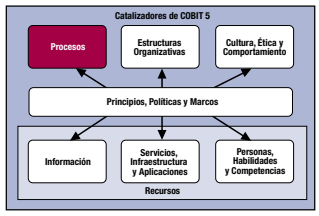
Esta sección trata sobre las políticas que son relevantes en un contexto de seguridad de la información, pero que no están desarrolladas o no pertenecen a la función de seguridad de la información. No obstante, para estas políticas, se requiere la opinión de la función de seguridad de la información. En la **figura 23**, se describe un posible alcance relevante para la función de seguridad de la información.

Figura 23—Políticas Específicas de Seguridad de la Información Dirigidas por Otras Funciones Dentro de la Organización: Alcance

Política	Alcance para la Función de Seguridad de la Información
Política de continuidad de negocio y recuperación de desastres	• Análisis de impacto en el negocio (BIA) • Planes de contingencia de negocio con la recuperación contrastada • Requisitos de recuperación para los sistemas críticos • Umbrales definidos y disparadores para contingencias y escalado de incidentes • Plan de recuperación de desastres (DRP) • Formación y pruebas
Política de gestión de activos	• Clasificación de la información • Propiedad de la información • Clasificación y propiedad de los sistemas • Utilización y priorización de recursos • Gestión del ciclo de vida de activos • Medidas de protección de activos

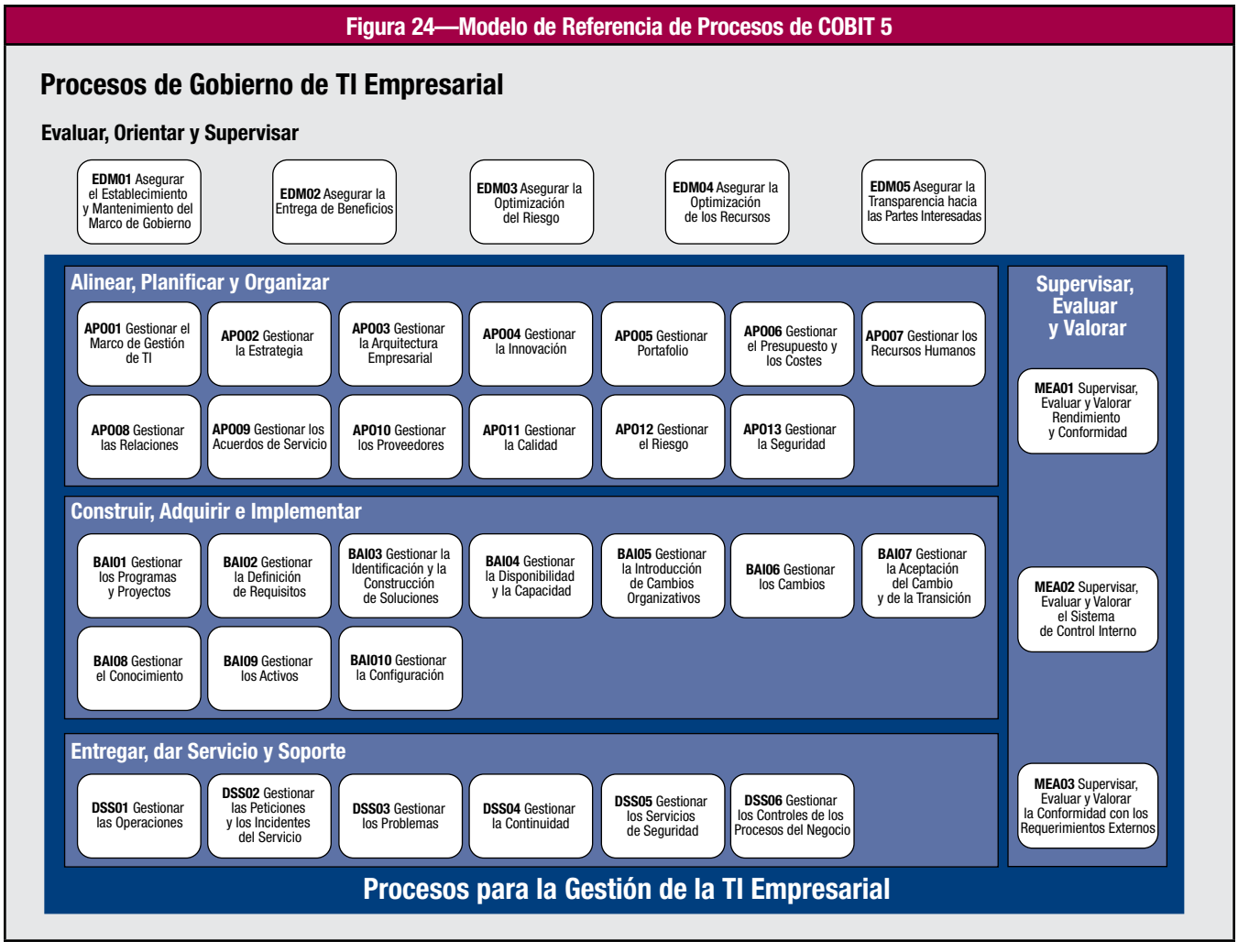
Figura 23—Políticas Específicas de Seguridad de la Información Dirigidas por Otras Funciones Dentro de la Organización: Alcance *(cont.)*	
Política	**Alcance para la Función de Seguridad de la Información**
Reglas de conducta (uso apropiado)	• Uso y comportamiento apropiados en el trabajo: – Expectativa de privacidad – Uso de los sistemas y activos de la empresa – Internet – Email – Mensajería instantánea – Acceso remoto – Uso de dispositivos móviles y cámaras – Utilización de impresora, escáner y fax – Uso de ordenadores particulares para actividades corporativas • Uso y comportamiento apropiados fuera de las instalaciones: – Redes sociales – Bitácoras personales
Política de adquisición, desarrollo y mantenimiento de de sistemas de información	• Seguridad de la información en el proceso de ciclo de vida • Seguridad de la información en el proceso de definición de los requisitos • Seguridad de la información en los procesos de compra/adquisición • Prácticas de programación segura • Integración de la seguridad de la información con la gestión de cambios y configuraciones
Política de gestión de proveedores	• Gestión de contratos: – Términos y condiciones referentes a la seguridad de la información. – Evaluación de la seguridad de la información – Supervisión de los contratos para el cumplimiento de la seguridad de la información
Política de gestión de las comunicaciones y las operaciones	• Diseño de arquitecturas y aplicaciones referentes a la seguridad de la información de TI: – Comité Directivo – Normas – Directrices • ANS: – Operaciones internas – Operaciones externas • Procedimientos operativos de seguridad de Información de TI
Política de cumplimiento	• Proceso de evaluación del cumplimiento de la seguridad de la información de TI: – Regulatoria – Contractual – Corporativa • Desarrollo de métricas • Repositorios de evaluación: – Audiencia – Contenido – Estructura – Seguimiento
Política de gestión de riesgos	• Plan de gestión del riesgo corporativo: – Alcance – Roles y responsabilidades – Metodologías – Técnicas y herramientas – Procesos del repositorio • Perfil de riesgo de la información

Apéndice B
Guía Detallada: Catalizador de Procesos



Los detalles de todos los procesos específicos de la seguridad de la información, de acuerdo con el modelo de procesos descrito en la sección II, se incluyen en *COBIT 5 para Seguridad de la Información* (véase la **figura 24**).

Figura 24—Modelo de Referencia de Procesos de COBIT 5



Página dejada en blanco intencionadamente

B.1 Evaluar, Orientar y Supervisar (EDM)

01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.

02 Asegurar la entrega de beneficios.

03 Asegurar la optimización del riesgo.

04 Asegurar la optimización de recursos.

05 Asegurar la transparencia hacia las partes interesadas.

Página dejada en blanco intencionadamente

EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	Área: Gobierno Dominio: Evaluar, Orientar y Supervisar
Descripción del Proceso de COBIT 5 Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.	
Declaración del Propósito del Proceso de COBIT 5 Proporcionar un enfoque consistente, integrado y alineado con el enfoque del gobierno de la empresa. Para garantizar que las decisiones relativas a TI se han adoptado en línea con las estrategias y objetivos de la empresa, garantizando la supervisión de los procesos de manera efectiva y transparentemente, el cumplimiento con los requerimientos regulatorios y legales y que se han alcanzado los requerimientos de gobierno de los miembros del Consejo de Administración.	
EDM01 Metas y métricas del proceso específicas de seguridad	
Metas del proceso específicas de seguridad	**Métricas relacionadas**
1. El sistema de gobierno de seguridad de la información está integrado en la empresa.	• Número de procesos de negocio y de TI en los que la seguridad de la información está integrada • Porcentaje de procesos y prácticas con clara trazabilidad a los principios • Número de brechas de seguridad de la información relativas a no conformidades con las directrices de comportamiento ético y profesional
1. Se obtiene garantía sobre el sistema de gobierno de la seguridad de la información.	• Frecuencia de revisiones independientes del gobierno de la seguridad de la información • Frecuencia de los informes sobre el gobierno de la seguridad de la información al comité ejecutivo y al consejo de administración • Número de auditorías y revisiones internas/externas • Número de no-conformidades

EDM01 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gobierno	**Desde**	**Descripción**	**Descripción**	**Hacia**
EDM01.01 Evaluar el sistema de gobierno. Identificar y comprometerse continuamente con las partes interesadas de la empresa, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del gobierno de TI de la empresa.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Factores internos y externos del entorno (obligaciones legales, regulatorias y contractuales) y tendencias	Principios que rigen la seguridad de la información	EDM01.02 APO01.01 APO01.03 APO01.04 APO02.01 APO02.05 APO12.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Analizar e identificar los factores del entorno internos y externos (obligaciones legales, regulatorias y contractuales) y las tendencias en el entorno del negocio que pueden influir en el diseño del gobierno de la seguridad de la información.				
2. Evaluar el grado en el que la seguridad de la información cumple con las necesidades de negocio y regulatorias/cumplimiento.				
3. Articular los principios que guiarán el diseño de los catalizadores de la seguridad de la información y promoverán un entorno positivo de seguridad.				
4. Comprender la cultura empresarial de la toma de decisiones y determinar el modelo óptimo de toma de decisiones para seguridad de la información.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gobierno	**Desde**	**Descripción**	**Descripción**	**Hacia**
EDM01.02 Orientar el sistema de gobierno. Informar a los líderes y obtener su apoyo, su aceptación y su compromiso. Guiar las estructuras, procesos y prácticas para el gobierno de TI en línea con los principios, modelos para la toma de decisiones y niveles de autoridad diseñados para el gobierno. Definir la información necesaria para una toma de decisiones informadas.	EDM01.01	Principios que rigen la seguridad de la información	Cultura y entorno positivo de seguridad de la información	Interno
	APO02.05	Estrategia de seguridad de la información		
Actividades específicas de seguridad (Adicionales a las Actividades de COBIT 5)				
1. Obtener el compromiso de la alta dirección con la seguridad de la información y la gestión de riesgos de la información.				
2. Asignar una función de seguridad de la información de alcance global dentro de la empresa.				
3. Asignar un comité de dirección de seguridad de la información (ISSC).				
4. Disponer procedimientos jerárquicos de notificación y de escalado de decisiones.				
5. Alinear la estrategia de seguridad de la información con la estrategia del negocio.				
6. Fomentar un entorno y cultura positivos de seguridad de la información.				

EDM01 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gobierno	**Desde**	**Descripción**	**Descripción**	**Hacia**
EDM01.03 Supervisar el sistema de gobierno. Supervisar la ejecución y la efectividad del gobierno de TI de la empresa. Analizar si el sistema de gobierno y los mecanismos implementados (incluyendo estructuras, principios y procesos) están operando de forma efectiva y proporcionan una supervisión apropiada de TI.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Legislación y regulación relacionada con la seguridad de la información	Evaluación de cumplimiento del sistema de gobierno	Interno
Actividades específicas de seguridad (Adicionales a las Actividades de COBIT 5)				
1. Supervisar los mecanismos ordinarios y rutinarios para garantizar que el uso de los sistemas de medida de la seguridad de la información cumplen con la legislación y regulación relacionada con la seguridad de la información. Analizar la totalidad de las implicaciones del cambiante contexto de las amenazas.				

Para más información relacionada con otros catalizadores afines, por favor consulte:
- Apéndice D. Guía Detallada: Catalizador de Cultura, Ética y Comportamiento
- Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias, G1. Gobierno de la seguridad de la información

EDM02 Asegurar la Entrega de Beneficios	Área: Gobierno Dominio: Evaluar, Orientar y Supervisar
Descripción del Proceso de COBIT 5 Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables	
Declaración del Propósito del Proceso de COBIT 5 Asegurar un valor óptimo de las iniciativas de TI, servicios y activos disponibles; una entrega coste eficiente de los servicios y soluciones y una visión confiable y precisa de los costes y de los beneficios probables de manera que las necesidades del negocio sean soportadas efectiva y eficientemente.	

EDM02 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	**Métricas Relacionadas**
1. Los beneficios, costes y riesgos de las inversiones en seguridad de la información son equilibradas y gestionadas y contribuyen en su valor óptimo.	• Porcentaje de reducción del riesgo frente a desviación del presupuesto (presupuestado frente a proyección) • Nivel de satisfacción de las partes interesadas con las medidas relativas a seguridad de la información existentes, basado en encuestas

EDM02 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad

Práctica de Gobierno	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
EDM02.01 Evaluar la optimización de valor. Evaluar continuamente las inversiones, servicios y activos del portafolio de TI para determinar la probabilidad de alcanzar los objetivos de la empresa y aportar valor a un coste razonable. Identificar y juzgar cualquier cambio de directrices que necesite ser comunicado a la dirección ejecutiva para optimizar la creación de valor.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Evaluación del alineamiento estratégico	Portafolio actualizado	Interno
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
1. Identificar y registrar los requisitos de las partes interesadas (tales como accionistas, reguladores, auditores y clientes) para proteger sus intereses y aportar valor a través de la actividad de seguridad de la información. Establecer directrices en consonancia con lo anterior.				
Práctica de Gobierno	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
EDM02.02 Orientar la optimización del valor. Orientar los principios y las prácticas de gestión de valor para posibilitar la materialización del valor óptimo de las inversiones habilitadas por TI a lo largo de todo su ciclo de vida económico.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Tipos y criterios de inversión	Tipos y criterios de inversión actualizados	Interno
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
1. Establecer un método para demostrar el valor de la seguridad de la información (incluyendo la definición y recolección de datos relevantes) para asegurar el uso eficiente de los activos existentes relacionados con la seguridad de la información.				
2. Asegurar el uso de medidas financieras y no financieras para describir el valor aportado por las iniciativas de seguridad de la información.				
3. Usar métodos enfocados al negocio para la comunicación del valor aportado por las iniciativas de seguridad de la información.				
Práctica de Gobierno	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
EDM02.03 Supervisar la optimización de valor. Supervisar los indicadores clave y sus métricas para determinar el grado en que el negocio está obteniendo el valor y los beneficios esperados de los servicios e inversiones habilitadas por TI. Identificar los problemas significativos y considerar las acciones correctivas.			Retroalimentación sobre el valor aportado por las iniciativas de seguridad de la información	Interno
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
1. Seguir los resultados de las iniciativas de seguridad de la información y compararlos con las expectativas para asegurar la entrega de valor frente a los objetivos del negocio.				

Para más información sobre los catalizadores relacionados, consulte:
- Sección II, 6. Catalizador: Información 6.3. Partes interesadas en la Información
- Apéndice E. Guía Detallada: Catalizador de Información

Página dejada en blanco intencionadamente

EDM03 Asegurar la Optimización del Riesgo	Área: Gobierno Dominio: Evaluar, Orientar y Supervisar
Descripción del Proceso de COBIT 5 Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.	
Declaración del Propósito del Proceso de COBIT 5 Asegurar que los riesgos relacionados con TI de la empresa no exceden los niveles de tolerancia o aversión al riesgo, que el impacto de los riesgos de TI en el valor de la empresa se identifica y se gestiona y que el potencial fallo en el cumplimiento se reduce al mínimo	

EDM03 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	**Métricas Relacionadas**
1. La gestión del riesgo asociado a la información forma parte de la gestión general de los riesgos corporativos (ERM).	• Porcentaje de riesgo de seguridad de la información relacionado con riesgo del negocio • Porcentaje de riesgo de negocio eficazmente mitigado con controles de seguridad de la información

EDM03 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad

Práctica de Gobierno	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
EDM03.01 Evaluar la gestión de riesgos. Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y si el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	• Indicadores clave del riesgo de la empresa (KRIs) • Orientación sobre apetito de riesgo de la empresa	Alineamiento de los KRIs de la empresa con los KRIs de seguridad de la información	EDM03.02
			Nivel aceptable del riesgo de seguridad de la información	EDM03.02 EDM03.03
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
1. Determinar el apetito de riesgo corporativo al nivel del consejo de administración.				
2. Medir el nivel de integración de la gestión del riesgo de la información con el modelo general de ERM.				

Práctica de Gobierno	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
EDM03.02 Orientar la gestión de riesgos. Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que el riesgo TI actual no excede el apetito de riesgo del consejo de administración.	EDM03.01	• Alineamiento de los KRIs de la empresa con los KRIs de seguridad de la información • Nivel aceptable del riesgo de seguridad de la información	Políticas de gestión del riesgo actualizadas	Interno
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
1. Integrar la gestión del riesgo de la información con el modelo general de ERM.				

Práctica de Gobierno	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
EDM03.03 Supervisar la gestión de riesgos. Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución.	EDM03.01	Nivel aceptable del riesgo de seguridad de la información	Acciones correctivas para solventar las desviaciones en la gestión del riesgo	Interno
	APO01.03	Políticas de Seguridad de la información y relacionadas		
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
1. Supervisar el perfil del riesgo de la información de la compañía o el apetito de riesgo, para conseguir un equilibrio óptimo entre riesgos y oportunidades de negocio.				
2. Incluir los resultados de los procesos de gestión del riesgo de la información como entradas para el cuadro de mando de riesgos general de negocio.				

Para más información sobre los catalizadores relacionados, consulte:
- Apéndice C. Guía Detallada: Catalizador de Estructuras Organizativas, C.4. Comité de Gestión de Riesgo Corporativo
- Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias, G.3. Gestión del Riesgo de la Información

Página dejada en blanco intencionadamente

EDM04 Asegurar la Optimización de Recursos	Área: Gobierno Dominio: Evaluar, Orientar y Supervisar
Descripción del Proceso de COBIT 5 Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.	
Declaración del Propósito del Proceso de COBIT 5 Asegurar que las necesidades de recursos de la empresa son cubiertas de un modo óptimo, que el coste TI es optimizado y que con ello se incrementa la probabilidad de la obtención de beneficios y la preparación para cambios futuros.	

EDM04 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	**Métricas Relacionadas**
1. Los recursos de seguridad de la información son optimizados.	• Estudio comparativo del gasto en seguridad de la información en relación a años anteriores y/u organizaciones similares o buenas prácticas del sector.
2. Los recursos de la seguridad de la información están alineados con los requisitos del negocio.	• Cuantía de la desviación respecto al presupuesto para seguridad de la información • Porcentaje de reutilización de soluciones de seguridad de la información

EDM04 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad

Práctica de Gobierno	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
EDM04.01 Evaluar la gestión de recursos. Examinar y evaluar continuamente la necesidad actual y futura de los recursos relacionados con TI, las opciones para la asignación de recursos (incluyendo estrategias de aprovisionamiento) y los principios de asignación y gestión para cumplir de manera óptima con las necesidades de la empresa.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Plan de recursos aprobado	Recursos de seguridad de la información actualizados	Interno
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
1. Evaluar la eficacia de los recursos de seguridad de la información en términos de suministro, formación, concienciación y competencias de los recursos necesarios en comparación con las necesidades del negocio.				
Práctica de Gobierno	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
EDM04.02 Orientar la gestión de recursos. Asegurar la adopción de principios de gestión de recursos para permitir un uso óptimo de los recursos de TI a lo largo de su completo ciclo de vida económica.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Asignación de responsabilidades para la gestión de recursos	Recursos de seguridad de la información actualizados	Interno
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
1. Asegurar que la gestión de los recursos de seguridad de la información está alineada con las necesidades del negocio.				
Práctica de Gobierno	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
EDM04.03 Supervisar la gestión de recursos. Supervisar los objetivos y métricas clave de los procesos de gestión de recursos y establecer cómo serán identificados, seguidos e informados para su resolución las desviaciones o los problemas.			Acciones correctivas para solventar las desviaciones en la gestión de los recursos	Interno
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
1. Medir la eficacia, eficiencia y capacidad de los recursos de seguridad de la información respecto a las necesidades del negocio.				

Para más información sobre los catalizadores relacionados, consulte:
• Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias

Página dejada en blanco intencionadamente

EDM05 Asegurar la Transparencia hacia las Partes Interesadas	Área: Gobierno Dominio: Evaluar, Orientar y Supervisar
Descripción del Proceso de COBIT 5 Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa son transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.	
Declaración del Propósito del Proceso de COBIT 5 Asegurar que la comunicación con las partes interesadas sea efectiva y oportuna y que se ha establecido una base para la elaboración de informes con el fin de aumentar el desempeño, identificar áreas susceptibles de mejora y confirmar que las estrategias y los objetivos relacionados con TI concuerdan con la estrategia corporativa.	
EDM05 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	**Métricas Relacionadas**
1. Se ha establecido un protocolo informativo completo, oportuno y preciso sobre la seguridad de la información.	• Porcentaje de informes entregados dentro del plazo previsto. • Porcentaje de informes con datos validados.
2. Las partes interesadas se encuentran informadas de la situación actual de la seguridad y de los riesgos de la información de toda la organización.	• Grado de satisfacción de las partes interesadas con el protocolo informativo sobre la seguridad de la información (oportuno, completo, relevante, fiable, preciso, etc.) y su frecuencia, basado en encuestas.

EDM05 Prácticas, Entradas /Salidas y Actividades del Proceso específicas de Seguridad				
Práctica de Gobierno	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas. Examinar y juzgar continuamente los requisitos actuales y futuros de comunicación con las partes interesadas y de la elaboración de informes, incluyendo tanto los requisitos obligatorios (p.ej. de regulación) de elaboración de informes, como la comunicación a otros interesados. Establecer los principios de la comunicación.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Evaluación de los requisitos corporativos de elaboración de informes	Requisitos de elaboración de informes y canales de comunicación de Seguridad de la Información	Interno
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
1. Determinar la audiencia, incluyendo individuos y grupos internos o externos, para la comunicación y elaboración de informes.				
2. Identificar los requisitos para la elaboración de informes de seguridad de la información a las partes interesadas (p.ej., qué información es requerida, cuándo es requerida y cómo es presentada).				
3. Identificar los medios y canales para comunicar los asuntos relativos a la Seguridad de la Información.				
Práctica de Gobierno	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes. Garantizar el establecimiento de una comunicación y una elaboración de informes eficaces, incluyendo mecanismos para asegurar la calidad y la completitud de la información, vigilar la elaboración obligatoria de informes y crear una estrategia de comunicación con las partes interesadas.			Informes de estado de la Seguridad de la Información	Interno
Actividades específicas de Seguridad (Además de las Actividades de COBIT 5)				
1. Priorizar la notificación de problemas de seguridad de la información a las partes interesadas.				
2. Realizar auditorías internas y externas para evaluar la eficacia del programa de gobierno de la seguridad de la información.				
3. Elaborar informes de estado de la seguridad de la información de forma regular para las partes interesadas que incluyan información de las actividades de seguridad, desempeño, logros, perfiles de riesgo, beneficios de negocio, temas 'calientes' (p.ej. computación en la nube, productos de consumo) riesgos destacados (incluyendo cumplimiento y auditoría) e insuficiencias de capacidad.				

EDM05 Prácticas, Entradas /Salidas y Actividades del Proceso específicas de Seguridad *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gobierno	**Desde**	**Descripción**	**Descripción**	**Hacia**
EDM05.03 Supervisar la comunicación con las partes interesadas. Supervisar la eficacia de la comunicación con las partes interesadas. Evaluar los mecanismos para asegurar la precisión, la fiabilidad y la eficacia y determinar si se están cumpliendo los requisitos de los diferentes interesados.			Supervisión y elaboración de informes de Seguridad de la Información	Interno
Actividades específicas de Seguridad (Además a las Actividades de COBIT 5)				
1. Definir la supervisión y elaboración de informes de seguridad de la información (p.ej., utilizando indicadores clave de desempeño [KPIs] para la seguridad de la información y la gestión de riesgos de la información que estén basados en métricas y medidas del dominio MEA)				

Para más información sobre catalizadores relacionados, por favor consultar:
- Sección II, 6. Catalizador: Información, 6.3.Información a las partes interesadas
- Apéndice E. Guía Detallada: Catalizador de Información

B.2 Alinear, Planificar y Organizar (APO)

01 Gestionar el marco de gestión de TI.

02 Gestionar la estrategia.

03 Gestionar la arquitectura empresarial.

04 Gestionar la innovación.

05 Gestionar el portafolio.

06 Gestionar el presupuesto y los costes.

07 Gestionar los recursos humanos.

08 Gestionar las relaciones.

09 Gestionar los acuerdos de servicio.

10 Gestionar los proveedores.

11 Gestionar la calidad.

12 Gestionar el riesgo.

13 Gestionar la seguridad.

Página dejada en blanco intencionadamente

APO01 Gestionar el Marco de Gestión de TI	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso de COBIT 5 Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.	
Declaración del Propósito del Proceso de COBIT 5 Proporcionar un enfoque de gestión consistente que permita cumplir los requisitos de gobierno corporativo e incluya procesos de gestión, estructuras, roles y responsabilidades organizativos, actividades fiables y reproducibles y habilidades y competencias.	

APO01 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	**Métricas Relacionadas**
1. Se ha establecido y comunicado eficazmente el alineamiento de la seguridad de la información con los marcos de TI y de negocio que operan en la empresa.	• Porcentaje de actividades de apoyo al alineamiento dentro del portafolio de la estrategia de seguridad de la información que resultan alineadas con la estrategia de negocio.

APO01 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad				
Práctica de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO01.01 Definir la estructura organizativa. Establecer una estructura organizativa interna y extensa que refleje las necesidades del negocio y las prioridades de TI. Implementar las estructuras de dirección requeridas (p. ej., comités) para permitir que la toma de decisiones de gestión se lleve a cabo de la forma más eficaz y eficiente posible.	EDM01.01	Principios que rigen la seguridad de la información	Estructura y mandato del ISSC	Interna
	Fuera del *ámbito de COBIT 5 para Seguridad de la Información*	• Estrategia de TI • Normas y directrices de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Alinear la organización relativa a la seguridad de la información con los modelos organizativos de arquitectura de empresa.				
1. Establecer un ISSC (o equivalente).				
1. Definir la función de seguridad de la información, incluyendo roles internos y externos, capacidades y derechos de decisión requeridos.				
Práctica de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO01.02 Establecer roles y responsabilidades. Establecer, acordar y comunicar roles y responsabilidades del personal de TI, así como de otras partes interesadas con responsabilidades en las TI corporativas, que reflejen claramente las necesidades generales del negocio y los objetivos de TI, así como la autoridad, las responsabilidades y la rendición de cuentas del personal relevante.	APO13.01	Declaración del alcance del sistema de gestión de seguridad de la información (SGSI)	Definición de los roles y responsabilidades relacionados con TI	DSS05.04
	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	• Regulaciones aplicables • Normas y directrices de seguridad de la información	Definiciones de los puestos de director de seguridad de la información (CISO) y de gerente de seguridad de la información (ISM)	Interna
	Modelo del catalizador "Principios y política"	Políticas de recursos humanos (RR.HH.) y legal		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Establecer, acordar y comunicar los roles de CISO y de ISM (o equivalentes).				
2. Determinar el grado en que otros roles organizativos tienen obligaciones en seguridad de la información y añadirlas a las descripciones de puesto correspondientes.				

APO01 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO01.03 Mantener los catalizadores del sistema de gestión. Mantener los catalizadores del sistema de gestión y del entorno de control para las TI de la empresa y garantizar que están integrados y alineados con la filosofía y el estilo operativo de gobierno y de gestión de la empresa. Dichos catalizadores incluyen una comunicación clara de expectativas/requisitos. El sistema de gestión debería fomentar la cooperación interdepartamental y el trabajo en equipo, promover el cumplimiento y la mejora continua y tratar las desviaciones en el proceso (incluidos los fallos).	EDM01.01	Principios que rigen la seguridad de la información	Políticas de seguridad de la información y afines	EDM03.03 APO07.01 APO07.06 APO12.01 BAI01.01 BAI01.11 BAI02.01 BAI03.08 BAI05.01 BAI06.01 DSS01.02 DSS02.01 MEA01.01 MEA02.01
	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	• Reglas y regulaciones relativas a la seguridad de la información • Normas y directrices de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Considerar el entorno interno de la empresa, incluyendo la cultura y la filosofía de la gestión, la tolerancia al riesgo, los valores éticos, el código de conducta, la rendición de cuentas y los requisitos de seguridad de la información.				
2. Alinearse con las normas y códigos de buenas prácticas de seguridad de la información aplicables, nacionales e internacionales, y evaluar las buenas prácticas disponibles de seguridad de la información.				
3. Desarrollar políticas de seguridad de la información y afines, teniendo en cuenta los requisitos de negocio, y los legales o regulatorios, y las obligaciones contractuales de seguridad, las políticas organizativas de alto nivel y el entorno interno de la empresa.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO01.04 Comunicar los objetivos y la dirección de gestión. Comunicar la sensibilización y la comprensión de los objetivos y la dirección de TI a las partes interesadas y usuarios pertinentes a lo largo de toda la empresa.	EDM01.01	Principios que rigen la seguridad de la información	Programa de formación y concienciación en seguridad de la información	APO02.06 BAI08.01
	APO02.06	Comunicación de los objetivos de la seguridad de la información		
	DSS05.01	Política de prevención de *software* malicioso		
	DSS05.02	Política de seguridad de las comunicaciones		
	DSS05.03	Políticas de seguridad para dispositivos de usuario		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir las expectativas en relación a la seguridad de la información, incluyendo la ética y la cultura específica de la organización.				
2. Desarrollar un programa de concienciación en seguridad de la información.				
3. Establecer métricas para medir los comportamientos en relación a la seguridad de la información.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO01.05 Optimizar la ubicación de la función de TI. Posicionar la capacidad de TI en la estructura organizativa global para reflejar un modelo de empresa acorde a la importancia de las TI en la organización, específicamente su criticidad para la estrategia corporativa y el nivel de dependencia de las TI. La línea de dependencia del CIO debe ser proporcional a la importancia de las TI en la empresa.			Definición de la función de seguridad de la información y su ubicación en la empresa	APO01.06
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir la función de seguridad de la información y todas las actividades y los atributos pertinentes.				
2. Definir la ubicación de la función de seguridad de la información en la empresa y obtener el acuerdo de todas las partes implicadas.				

APO01 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO01.06 Definir la propiedad de la información (datos) y de los sistemas. Definir y mantener las responsabilidades sobre la propiedad de la información (datos) y los sistemas de información. Asegurar que los propietarios toman decisiones sobre la clasificación de la información y los sistemas y sobre su protección de acuerdo con esta clasificación.	APO01.05	Definición de la función de seguridad de la información y su ubicación en la empresa	Roles y responsabilidades de seguridad de la información	APO11.01
			Directrices de clasificación de datos	DSS05.02
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir la propiedad de sistemas y datos al nivel de la empresa dentro de los procesos de gestión de seguridad de la información.				
2. Asignar custodios de seguridad de la información de datos en los procesos de gestión de seguridad de la información.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO01.07 Gestionar la mejora continua de los procesos. Evaluar, planificar y ejecutar la mejora continua de los procesos y su madurez, para asegurar que son capaces de entregarse conforme a los objetivos de la empresa, de gobierno, de gestión y de control. Considerar las directrices de la implementación de procesos de COBIT, los estándares emergentes, los requerimientos de cumplimiento, las oportunidades de automatización y la realimentación de los usuarios de los procesos, el equipo del proceso y otras partes interesadas. Actualizar los procesos y considerar el impacto sobre sus catalizadores.	MEA01.04	Informes de seguridad de la información y planes de acciones correctivas, actualizados	• Documentación sobre procesos, tecnología y aplicaciones y normalización • Formación del equipo de seguridad de la información	Interna
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Considerar formas de mejorar la eficiencia y la eficacia de la función de seguridad de la información, p.ej., mediante la formación del equipo de seguridad de la información; la documentación de procesos, tecnología y aplicaciones; y la normalización y la automatización del proceso.				
2. Revisar los informes (tales como los informes de auditoría y las evaluaciones de riesgo) que detallan las debilidades en los controles y procesos de seguridad de la información.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO01.08 Mantener el cumplimiento con las políticas y procedimientos. Poner en marcha procedimientos para mantener el cumplimiento y la medición del funcionamiento de las políticas y otros catalizadores del marco de referencia; hacer cumplir las consecuencias del no cumplimiento o del desempeño inadecuado. Hacer un seguimiento de las tendencias y del rendimiento y considerarlos en el diseño futuro y la mejora del marco de control.	APO02.05	Estrategia de seguridad de la información	Evaluación del cumplimiento de seguridad de la información	APO02.02 APO12.01
	APO02.06	Plan de seguridad de la información		
	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	• Objetivos de la organización • Reglas y regulaciones relativas a la seguridad de la información • Normas y directrices de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Planificar y realizar evaluaciones periódicas para determinar el cumplimiento de las políticas y procedimientos de seguridad de la información.				

Para más información sobre los catalizadores relacionados, consulte:
- Apéndice C. Guía Detallada: Catalizador de Estructuras Organizativas, C.1 Director de Seguridad de la Información (CISO), C.2. Comité de Supervisión de Seguridad de la Información (ISSC), C.3. Gerente

Página dejada en blanco intencionadamente

APO02 Gestionar la Estrategia	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso de COBIT 5 Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.	
Declaración del Propósito del Proceso de COBIT 5 Alinear los planes estratégicos de TI con los objetivos del negocio. Comunicar claramente los objetivos y las cuentas asociadas para que sean comprendidos por todos, con la identificación de las opciones estratégicas de TI, estructurados e integrados con los planes de negocio.	

APO02 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	**Métricas Relacionadas**
1. Se define y mantiene un marco de política de seguridad de la información.	• Número de actualizaciones de la política de seguridad de la información • Aprobación de la política de seguridad de la información por la Dirección
2. Existe una estrategia integral de seguridad de la información y está alineada con la estrategia general de la empresa y de TI.	• Porcentaje de iniciativas de seguridad de la información completadas frente a las planeadas
3. La estrategia de seguridad de la información es rentable, apropiada, realista, factible, orientada a la empresa y equilibrada.	• Porcentaje y número de iniciativas para las que se ha calculado una métrica de valor (p.ej., el retorno de la inversión [ROI]) • Datos de las encuestas de satisfacción de los grupos de interés de la empresa sobre la eficacia de la estrategia de seguridad de la información
4. La estrategia de seguridad de la información está alineada con las metas y objetivos estratégicos de la empresa a largo plazo	• Porcentaje de proyectos en los portafolios de proyectos de la empresa y de TI que incluyen seguridad de la información • Porcentaje de iniciativas/proyectos de TI en que los requisitos de seguridad de la información están promovidos por los propietarios de negocio

APO02 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad

Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO02.01 Comprender la dirección de la empresa. Considerar el entorno actual y los procesos de negocio de la empresa, así como la estrategia y los objetivos futuros de la compañía. Tomar también en cuenta el entorno externo a ella (catalizadores de la industria, regulaciones relevantes, bases para la competencia).	EDM01.01	Principios que rigen la seguridad de la información	Fuentes de alto nivel y prioridades para los cambios	APO02.02

Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)

1. Comprender cómo la seguridad de la información debería apoyar los objetivos generales de la empresa y proteger los intereses de las partes implicadas teniendo en cuenta la necesidad de gestionar el riesgo de la información, al tiempo que se cumplen los requisitos de conformidad legal y regulatoria y se aporta valor a la empresa.
2. Comprender la vigente arquitectura de empresa e identificar las deficiencias potenciales de seguridad de la información.

Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO02.02 Evaluar el entorno, capacidades y rendimiento actuales. Evaluar el rendimiento de las actuales capacidades internas de negocio y de TI, así como el de los servicios externos de TI; y desarrollar una perspectiva de la arquitectura empresarial en relación a TI. Identificar los problemas que se están experimentando y generar recomendaciones en las áreas que pueden beneficiarse de estas mejoras. Considerar los aspectos diferenciadores y las opciones de los proveedores de servicios, y el impacto financiero, los costes y beneficios potenciales de utilizar servicios externos.	APO01.08	Evaluación de cumplimiento de la seguridad de la información	Capacidades de seguridad de la información	APO02.03 APO04.04 APO08.05 APO09.05 APO11.01 BAI01.01 BAI02.01 BAI04.01
	APO02.01	Fuentes de alto nivel y prioridades para los cambios		

Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)

1. Definir unas capacidades básicas de seguridad de la información.
2. Crear criterios de seguridad de la información pertinentes y claros para identificar el riesgo y priorizar las deficiencias a tratar.

APO02 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad *(cont.)*				
Práctica de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO02.03 Definir las capacidades objetivo para TI. Definir las capacidades objetivo para el negocio y para TI y los servicios de TI necesarios. Esto debería estar basado en el entendimiento del entorno empresarial y sus necesidades; en la evaluación de los actuales procesos de negocio, el entorno de TI y los problemas presentados; considerando los estándares de referencia, las mejores prácticas y las tecnologías emergentes validadas o propuestas de innovación.	APO02.02	Capacidades de seguridad de la información	Necesidades de seguridad de la información en las capacidades objetivo para TI	APO02.04
	BAI02.01	Necesidades de seguridad de la información		
	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Normas y regulaciones de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Garantizar que los requisitos de seguridad de la información se incluyen en la definición de las capacidades objetivo para TI.				
2. Definir el estado objetivo para la seguridad de la información.				
3. Definir y consensuar el impacto de los requisitos de seguridad de la información en la arquitectura de la empresa, considerando a las partes interesadas pertinentes.				
Práctica de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO02.04 Realizar un análisis de las deficiencias. Identificar las diferencias entre el entorno actual y el deseado y considerar el alineamiento de activos (las capacidades que soportan los servicios) con los resultados del negocio para optimizar la inversión, y la utilización de la base de activos internos y externos. Considerar los factores críticos de éxito que apoyan la ejecución de la estrategia.	APO02.03	Necesidades de seguridad de la información en las capacidades objetivo para TI	Análisis comparativo de las capacidades en seguridad de la información	APO03.01
			Carencias que han de ser cubiertas y cambios requeridos para alcanzar la capacidad objetivo	APO13.02
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Identificar todas las carencias que han de ser cubiertas y los cambios requeridos para lograr el entorno deseado.				
2. Realizar un análisis comparativo de la seguridad de la información frente a normas del sector conocidas y fiables.				
3. Examinar el entorno actual con respecto a las regulaciones y los requisitos de cumplimiento.				
Práctica de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO02.05 Definir el plan estratégico y la hoja de ruta. Crear un plan estratégico que defina, en cooperación con las partes interesadas relevantes, cómo los objetivos de TI contribuirán a los objetivos estratégicos de la empresa. Incluyendo cómo TI apoyará el programa aprobado de inversiones, los procesos de negocio, los servicios y los activos de TI. Orientar las tecnologías para definir las iniciativas que se requieren para cubrir las diferencias, la estrategia de abastecimiento y las medidas que se utilizarán para supervisar el logro de los objetivos, para dar prioridad a las iniciativas y combinarlas en una hoja de ruta a alto nivel.	EDM01.01	Principios que rigen la seguridad de la información	Estrategia de seguridad de la información	EDM01.02 APO01.08 APO03.01
	APO13.02	Casos de negocio de seguridad de la información	Hoja de ruta estratégica de seguridad de la información	BAI05.04
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir la estrategia de seguridad de la información y alinearla con las estrategias de TI y de negocio y con los objetivos globales corporativos.				
2. Garantizar que la estrategia y la hoja de ruta actuales de TI tienen en consideración los requisitos de seguridad de la información.				
3. Crear un plan de acción que incluya una planificación tentativa, interdependencias entre las iniciativas y métricas (el qué) y objetivos (el cuánto) que puedan relacionarse con los beneficios corporativos.				

APO02 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO02.06 Comunicar la estrategia y la dirección de TI. Crear conciencia y comprensión del negocio y de los objetivos y dirección de TI, como se encuentra reflejada en la estrategia de TI, a través de comunicaciones a las partes interesadas actuales y a los usuarios de toda la empresa.	APO01.04	Programa de formación y concienciación en seguridad de la información	Comunicación de los objetivos de seguridad de la información	APO01.04
			Plan de seguridad de la información	APO01.08 APO04.04 APO04.05 APO07.01 APO07.05 APO07.06 APO09.05 APO11.01 BAI01.01 BAI01.04 BAI01.08 BAI01.11 BAI02.01 BAI05.03 BAI05.04
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir el plan de seguridad de la información, identificando las consecuencias prácticas para la empresa de la seguridad de la información.				
2. Comunicar la estrategia de seguridad de la información y el plan de seguridad de la información a la empresa y a todas las partes interesadas pertinentes.				
3. Dar a conocer la función de seguridad de la información dentro de la empresa, y fuera de ella si es pertinente.				

Para más información sobre catalizadores relacionados, por favor consúltese:
- Apéndice E. Guía Detallada: Catalizador de Información, E.2. Estrategia de Seguridad de la Información
- Apéndice G. Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias, G.4. Desarrollo de la Arquitectura de Seguridad de la Información

Página dejada en blanco intencionadamente

APO03 Gestionar la Arquitectura Empresarial	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso de COBIT 5 Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Definir los requisitos para la taxonomía, las normas, las directrices, los procedimientos, las plantillas y las herramientas y proporcionar un vínculo para estos componentes. Mejorar la adecuación, aumentar la agilidad, mejorar la calidad de la información y generar ahorros de costes potenciales mediante iniciativas tales como la reutilización de bloques de componentes para los procesos de construcción.	
Declaración del Propósito del Proceso de COBIT 5 Representar a los diferentes módulos que componen la empresa y sus interrelaciones, así como los principios rectores de su diseño y evolución en el tiempo, permitiendo una entrega estándar, sensible y eficiente de los objetivos operativos y estratégicos.	

APO03 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	**Métricas Relacionadas**
1. Los requisitos de seguridad de la información se han incorporado a la arquitectura de la empresa y se han traducido en una arquitectura de seguridad formalizada.	• Número de excepciones a los estándares de arquitectura de seguridad de la información
2. La arquitectura de seguridad de la información se entiende como parte de la arquitectura general de la empresa.	• Número de desviaciones entre la arquitectura de seguridad de la información y la arquitectura de la empresa
3. La arquitectura de seguridad de la información está alineada con la arquitectura de la empresa y evoluciona según cambia ésta.	• Fecha de la última revisión y/o actualización de los controles de seguridad de la información aplicados a la arquitectura de la empresa
4. Se utilizan un marco y una metodología de arquitectura de seguridad de la información para permitir la reutilización de componentes de seguridad de la información entre distintas partes de la empresa.	• Porcentaje de proyectos que utilizan el marco y la metodología de arquitectura de seguridad de la información • Número de personas formadas en el marco y la metodología de seguridad de la información

APO03 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad

Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO03.01 Desarrollar la visión de la arquitectura de empresa. La visión de la arquitectura proporciona una primera descripción de alto nivel de las arquitecturas de partida y objetivo, cubriendo los dominios de negocio, información, datos, aplicaciones y tecnología. La visión de la arquitectura proporciona al promotor la herramienta clave para vender los beneficios de la capacidad propuesta a las partes interesadas de la empresa. La visión de la arquitectura describe cómo las nuevas capacidades permitirán alcanzar las metas de la empresa y los objetivos estratégicos y considera las preocupaciones de las partes interesadas en su implementación.	APO02.04	Análisis comparativo de la capacidad de seguridad de la información	• Visión de arquitectura de seguridad de la información • Propuesta de valor, metas y métricas de seguridad de la información	Interno
	APO02.05	Estrategia de seguridad de la información		

Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)
1. Definir los objetivos y requisitos de seguridad de la información para la arquitectura de empresa.
2. Definir la propuesta de valor de la seguridad de la información así como las metas y métricas afines.
3. Tener en cuenta las buenas prácticas del sector al construir la visión de la arquitectura de seguridad de la información.

Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO03.02 Definir la arquitectura de referencia. La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Arquitectura de empresa	Definición de la arquitectura deseada de la seguridad de la información	APO03.03
			Descripciones de partida de los dominios y definición de la arquitectura	APO13.02
			Modelo de la arquitectura de la información	DSS05.03 DSS05.04 DSS05.06

Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)
1. Asegurar la inclusión de elementos, políticas y normas de seguridad de la información en el repositorio de arquitectura.
2. Asegurar que la seguridad de la información se encuentra integrada a lo largo de todos los dominios de la arquitectura (p. ej., negocio, información, datos, aplicaciones, tecnología).

APO03 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO03.03 Seleccionar las oportunidades y las soluciones. Racionalizar las desviaciones entre las arquitecturas de referencia y objetivo, considerando tanto la perspectiva técnica como la del negocio y agrupándolas en paquetes de trabajo de proyecto. Integrar el proyecto con todos los programas de inversiones relacionados con TI para asegurar que las iniciativas relacionadas con la arquitectura estén alineadas y que, estas iniciativas, sean parte del cambio general en la empresa. Hacer de ello un esfuerzo en colaboración con las partes interesadas clave de la empresa y en TI para evaluar el grado de preparación de la empresa para su transformación e identificar oportunidades, soluciones y todas las restricciones de la implementación.	APO03.02	Definición de la arquitectura deseada de seguridad de la información	Estrategia de migración y puesta en marcha de la arquitectura de seguridad de la información	APO03.04
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar la inclusión de los requisitos de seguridad de la información cuando se analicen carencias y cuando se seleccionen soluciones para la empresa.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO03.04 Definir la implementación de la arquitectura. Crear un plan de implementación y de migración viable, acorde con la cartera de proyectos y programas. Asegurar que el plan está estrechamente coordinado para asegurar que se aporta valor y se disponen de los recursos necesarios para finalizar los trabajos.	APO03.03	Estrategia de implementación y migración de la arquitectura de seguridad de la información	Arquitectura de seguridad de la información y plan de implementación del servicio detallados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Alinear la seguridad de la información con la arquitectura de TI.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO03.05 Proveer los servicios de arquitectura empresarial. La provisión de los servicios de arquitectura de empresa incluye la guía y supervisión de los proyectos a implementar, la formalización de las maneras de trabajar mediante los contratos de arquitectura, la medición y comunicación del valor añadido por la arquitectura y la supervisión del cumplimiento.			Guía para la puesta en marcha de servicios de arquitectura de seguridad de la información	DSS01.01
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir normas de seguridad de la información y diseñar patrones en apoyo a la arquitectura empresarial.				
2. Asegurar que cualquier adquisición tecnológica o actividad de cambio en el negocio incluye revisiones de seguridad de la información para confirmar que se cumplen los requisitos de seguridad de la información.				

Para más información sobre catalizadores relacionados, consúltese:
- Apéndice E. Guía Detallada: Catalizador de Información, E.2. Estrategia de Seguridad de la Información
- Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias, G.4. Desarrollo de la Arquitectura de Seguridad de la Información

APO04 Gestionar la Innovación	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso de COBIT 5 Mantener un conocimiento de la tecnología de la información y las tendencias relacionadas con el servicio, identificar las oportunidades de innovación y planificar la manera de beneficiarse de la innovación en relación con las necesidades del negocio. Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de TI. Influir en la planificación estratégica y en las decisiones de la arquitectura de empresa.	
Declaración del Propósito del Proceso de COBIT 5 Lograr ventaja competitiva, innovación empresarial y eficacia y eficiencia operativa mejorada mediante la explotación de los desarrollos tecnológicos para la explotación de la información.	

APO04 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	**Métricas Relacionadas**
1. Se promueve la innovación dentro del programa de seguridad de la información.	• Porcentaje del presupuesto asignado a investigación y desarrollo en seguridad de la información
2. Se tienen en cuenta los requisitos de seguridad de la información cuando se habilita la innovación.	• Número de puestos que incluyen aspectos de innovación

APO04 Security-specific Process Practices, Inputs/Outputs and Activities

Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO04.01 Crear un entorno favorable para la innovación. Crear un entorno que sea propicio para la innovación, considerando la cultura, la gratificación, la colaboración, los foros tecnológicos y los mecanismos para promover y captar ideas de los empleados.			Plan de innovación en seguridad de la información	APO04.06
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Mantener políticas y principios de seguridad de la información que respalden la innovación, al tiempo que se gestiona el riesgo de la información.				
2. Establecer enlaces con la investigación y otros servicios de asesoramiento en seguridad.				

Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO04.02 Mantener un entendimiento del entorno de la empresa. Trabajar junto a las partes interesadas relevantes para entender sus retos. Mantener un entendimiento adecuado de la estrategia corporativa y del entorno competitivo, así como de otras restricciones de modo que las oportunidades habilitadas por las nuevas tecnologías puedan ser identificadas.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Investigación externa	Evaluaciones de impacto de nuevas iniciativas en la seguridad de la información	Interna
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Comprender, en todo momento, los catalizadores de la seguridad de la información para identificar oportunidades y limitaciones de la innovación tecnológica.				
2. Determinar los efectos e impacto de las innovaciones en la tecnología, el entorno y la seguridad de la información.				

Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO04.03 Supervisar y explorar el entorno tecnológico. Realizar una supervisión sistemática y una exploración del entorno externo a la empresa para identificar tecnologías emergentes que tengan el potencial de crear valor (por ejemplo, materializando la estrategia corporativa, optimizando costes, evitando la obsolescencia y habilitando de una mejor manera los procesos corporativos y de TI). Supervisar el mercado, la competencia, sectores industriales y tendencias legales y regulatorias para poder analizar tecnologías emergentes o ideas innovadoras en el contexto empresarial.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Investigación externa	Tendencias emergentes identificadas en seguridad de la información	APO08.02
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Llevar a cabo investigación y una exploración del entorno externo para identificar tendencias emergentes en seguridad de la información.				
2. Fomentar la realimentación de las partes interesadas sobre la innovación en seguridad de la información.				

APO04 Security-specific Process Practices, Inputs/Outputs and Activities *(cont.)*				
Práctica de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO04.04 Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras. Analizar las tecnologías emergentes identificadas y/u otras sugerencias de innovación TI. Trabajar con las partes interesadas para validar los supuestos sobre el potencial de las nuevas tecnologías y la innovación.	APO02.02	Capacidades de la seguridad de la información	Evaluación del cumplimiento de los requisitos de seguridad de la información	APO04.05
	APO02.06	Plan de seguridad de la información		
	BAI02.01	Requisitos de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Evaluar las innovaciones identificadas en base a los catalizadores de seguridad de la información.				
2. Apoyar las actividades de prueba de concepto para iniciativas de innovación, con el objetivo de asegurar la cobertura de los requisitos de seguridad de la información. Evaluar el cumplimiento de estos requisitos.				
Práctica de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO04.05 Recomendar iniciativas apropiadas adicionales. Evaluar y supervisar los resultados de las pruebas de concepto y, si son favorables, generar recomendaciones para más iniciativas y obtener el soporte de las partes interesadas.	APO02.06	Plan de seguridad de la información	Recomendaciones en seguridad de la información a partir de los resultados de la prueba de concepto	Interna
	APO04.04	Evaluación del cumplimiento de los requisitos de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Proporcionar asesoramiento en seguridad de la información a partir de los resultados de las pruebas de concepto de iniciativas de innovación de TI.				
Práctica de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO04.06 Supervisar la implementación y el uso de la innovación. Supervisar la implementación y el uso de las tecnologías emergentes durante la integración, adopción y durante todo el ciclo de vida económico para garantizar que se producen los beneficios prometidos y para identificar las lecciones aprendidas.	APO04.01	Plan de innovación en seguridad de la información	Planes de innovación ajustados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Medir los beneficios y riesgos para la seguridad durante la prueba de concepto y otras actividades de innovación.				

APO05 Gestionar el Portafolio	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso de COBIT 5 Ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación. Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos así como en su valor y riesgo corporativo. Mover los programas seleccionados al portafolio de servicios activos listos para ser ejecutados. Supervisar el rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas.	
Declaración del Propósito del Proceso de COBIT 5 Optimizar el rendimiento del portafolio global de programas en respuesta al rendimiento de programas y servicios y a las cambiantes prioridades y demandas corporativas.	

APO05 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	**Métricas Relacionadas**
1. Las inversiones en seguridad de la información están asignadas según la tolerancia al riesgo.	• Número de casos de negocio de inversión en seguridad de la información que no realizan evaluaciones de riesgo
2. Los cambios en el programa de seguridad de la información se reflejan en los portafolios relevantes de servicios, activos y recursos de TI.	• Porcentaje de cambios del programa de seguridad de la información reflejado en los portafolios relevantes

APO05 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad

Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO05.01 Establecer la combinación deseada de inversiones. Revisar y garantizar la claridad de las estrategias y servicios actuales corporativos y de TI. Definir una adecuada combinación de inversiones, basada en los costes, la alineación con la estrategia y medidas financieras, tales como coste y retorno esperado de la inversión a lo largo de todo el ciclo de vida económico, grado de riesgo y tipo de beneficio para los programas del portafolio. Ajustar las estrategias corporativas y de TI cuando sea necesario.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Evaluación del riesgo	Combinación deseada de inversiones en seguridad de la información	APO05.02
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir la combinación deseada de inversiones en seguridad de la información, teniendo en cuenta el riesgo para la empresa, los beneficios financieros y no financieros y el potencial retorno de las iniciativas.				
Práctica de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO05.02 Determinar la disponibilidad y las fuentes de fondos. Determinar las fuentes potenciales de fondos, las diferentes opciones de financiación y las implicaciones de las fuentes de financiación sobre las expectativas de retorno de la inversión.	APO05.01	Combinación deseada de inversiones en seguridad de la información	Opciones de financiación	APO05.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Revisar las posibilidades internas y externas para cubrir los recursos necesarios de seguridad de la información.				
Práctica de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO05.03 Evaluar y seleccionar los programas a financiar. A partir de los requisitos de la combinación de inversiones del portafolio general, evaluar y priorizar casos de negocio de programas y decidir sobre las propuestas de inversión. Asignar fondos e iniciar los programas.	APO05.02	Opciones de financiación	Programa de seguridad de la información	Interna
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar la existencia de un programa de seguridad de la información.				

APO05 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO05.04 Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversión. Periódicamente, supervisar y optimizar, el rendimiento del portafolio de inversiones y de los programas individuales, a lo largo de todo el ciclo de vida de dichas inversiones.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No son necesarias guías específicas sobre seguridad de la información para esta práctica. Las actividades genéricas de COBIT 5 pueden ser utilizadas como guía adicional.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO05.05 Mantener los portafolios. Mantener los portafolios de programas y proyectos de inversión, servicios de TI y activos de TI.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No son necesarias guías específicas sobre seguridad de la información para esta práctica. Las actividades genéricas de COBIT 5 pueden ser utilizadas como guía adicional.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO05.06 Gestionar la consecución de beneficios. Supervisar los beneficios de proporcionar y mantener servicios y capacidades TI apropiadas, sobre la base del caso de negocio acordado en vigor.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Presupuesto del programa	Perfil actualizado del riesgo de seguridad de la información	Interna
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Proporcionar información sobre el logro de la confidencialidad, la integridad y la disponibilidad de la información, como entrada a la gestión de la consecución de beneficios.				
2. Evaluar los cambios en el perfil de riesgo de seguridad de la información, para ilustrar la consecución de beneficios.				

Para más información acerca de los catalizadores relacionados, por favor consulta:
- Apéndice E. Guía Detallada: Catalizador de Información, E.4. Plan de Seguridad de la Información

APO06 Gestionar el Presupuesto y los Costes	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso de COBIT 5 Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, coste y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costes a la empresa. Consultar a las partes interesadas para identificar y controlar los costes totales y los beneficios en el contexto de los planes estratégicos y tácticos de TI, e iniciar acciones correctivas cuando sea necesario.	
Declaración del Propósito del Proceso de COBIT 5 Fomentar la colaboración entre TI y las partes interesadas de la empresa para catalizar el uso eficaz y eficiente de los recursos relacionados con las TI y brindar transparencia y responsabilidad sobre el coste y valor de negocio de soluciones y servicios. Permitir a la empresa tomar decisiones informadas con respecto a la utilización de soluciones y servicios de TI.	

APO06 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	**Métricas Relacionadas**
1. La asignación de presupuestos y costes a seguridad de la información se prioriza de forma eficaz.	• Porcentaje de alineamiento entre los recursos de TI y las iniciativas importantes de control y seguridad de la información • Número de problemas en la asignación de recursos debidos a incidentes en seguridad de la información • Número de solicitudes de presupuesto adicional debidas a incidentes en seguridad de la información

APO06 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad

Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO06.01 Gestionar las finanzas y la contabilidad. Establecer y mantener un método de contabilización para todos los costes, inversiones y depreciaciones relacionadas con las TI, como parte integral de los sistemas financieros empresariales y un plan de cuentas para administrar las inversiones y los costes de TI. Capturar y asignar los costes reales, analizar las desviaciones entre las previsiones y los costes reales, e informar usando los sistemas empresariales de medición financiera.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No son necesarias guías específicas sobre seguridad de la información para esta práctica. Las actividades genéricas de COBIT 5 pueden ser utilizadas como guía adicional.				
Práctica de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO06.02 Priorizar la asignación de recursos. Implementar un proceso de toma de decisiones para priorizar la asignación de recursos y definir las reglas para las inversiones discrecionales realizadas, a título individual, por las unidades de negocio. Incluir el uso potencial de proveedores de servicio externos y considerar las opciones de compra, desarrollo y alquiler.			Priorización de las iniciativas.	APO06.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que cuando se prioriza la asignación de recursos, se tienen en consideración criterios para la priorización acordes a los perfiles de riesgo de la información.				
Práctica de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO06.03 Crear y mantener presupuestos. Preparar un presupuesto que refleje las prioridades de inversión que apoyen los objetivos estratégicos, tomando como base la cartera de programas habilitados por TI y de servicios de TI.	APO06.02	Priorización de las iniciativas	Presupuesto para la seguridad de la información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir un presupuesto para la seguridad de la información.				

APO06 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO06.04 Modelar y asignar costes. Establecer y utilizar un modelo de costes de TI basado en la definición del servicio, asegurando que la asignación de costes de los servicios es identificable, medible y predecible, para fomentar el uso responsable de los recursos, incluidos aquellos proporcionados por proveedores de servicio. Revisar y comparar periódicamente la idoneidad del modelo de costes/ prorrateo, para mantener su pertinencia y adecuación a las cambiantes actividades del negocio y de TI.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No son necesarias guías específicas sobre seguridad de la información para esta práctica. Las actividades genéricas de COBIT 5 pueden ser utilizadas como guía adicional.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO06.05 Gestionar costes. Poner en marcha un proceso de gestión de costes que compare los costes reales con los presupuestos. Los costes deben ser supervisados y comunicados y, en caso de desviaciones, identificados oportunamente, así como evaluado su impacto en los procesos y servicios empresariales.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No son necesarias guías específicas sobre seguridad de la información para esta práctica. Las actividades genéricas de COBIT 5 pueden ser utilizadas como guía adicional.				

APO07 Gestionar los Recursos Humanos	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso de COBIT 5 Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.	
Declaración del Propósito del Proceso de COBIT 5 Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa.	

APO07 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	**Métricas Relacionadas**
1. Las capacidades y procesos de recursos humanos están alineados con los requisitos de seguridad de la información.	• Porcentaje de empleados a los que se proporciona una iniciación en seguridad de la información • Tasa de rotación en seguridad de la información • Tiempo de ciclo de contratación o de incorporación • Cualificaciones del personal en términos de certificaciones, formación y años de experiencia

APO07 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad

Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO07.01 Mantener la dotación de personal suficiente y adecuada. Evaluar las necesidades de personal de forma regular o ante cambios importantes en la empresa, o en los entornos operativos o de TI, para asegurar que la empresa tiene suficientes recursos humanos para apoyar las metas y objetivos empresariales. El personal incluye recursos tanto internos como externos.	APO01.03	Políticas de seguridad de la información y otras afines	Requisitos de seguridad de la información para la dotación de personal de los procesos	Interna
	APO02.06	Plan de seguridad de la información		
	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Normativas locales		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que los requisitos de seguridad de la información asociados a dotar el proceso de personal , son incorporados en los procesos de contratación de TI para empleados, subcontratistas y proveedores.				
Práctica de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO07.02 Identificar personal clave de TI. Identificar al personal clave de TI a la vez que se reduce al mínimo las dependencias unipersonales en la realización de una función crítica de trabajo, mediante la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión y el respaldo del personal.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	• Lista de normativas internas y externas que afectan a las vacaciones y a otros derechos y obligaciones laborales • Análisis de impacto en el negocio (BIA) de los procesos de negocio • Lista de normativas internas y externas que afecten a la segregación de funciones y a las políticas de RRHH o de seguridad (personal) • Lista de funciones de negocio, roles y su rendimiento de cuentas y otras responsabilidades relacionadas con los procesos de negocio	• Lista de contactos de emergencia • Planes de sucesión	Interna
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar la segregación de funciones en los puestos críticos.				

APO07 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO07.03 Mantener las habilidades y competencias del personal. Definir y gestionar las habilidades y competencias necesarias del personal. Verificar regularmente que el personal tenga las competencias necesarias para cumplir con sus funciones sobre la base de su educación, formación y/o experiencia; y verificar que estas competencias se mantienen, con programas de capacitación y certificación en su caso. Proporcionar a los empleados formación continua y oportunidades para mantener sus conocimientos, habilidades y competencias al nivel requerido para conseguir las metas empresariales.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	• Listado del personal • Listado de contratistas • Habilidades del personal	Plan de formación en seguridad de la información	APO07.04
			Entrenamiento y concienciación en seguridad de la información	Interna
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Proporcionar formación y programas de desarrollo profesional sobre seguridad de la información.				
2. Hacer uso de los programas de certificación personal para asegurar un conjunto de habilidades profesionales, de calidad, en seguridad de la información.				
3. Establecer los oportunos programas educativos, de formación y de concienciación, de alcance corporativo, en seguridad de la información.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO07.04 Evaluar el desempeño laboral de los empleados. Lleve a cabo oportunamente evaluaciones de rendimiento de manera regular respecto a los objetivos individuales derivados de los objetivos de la empresa, a las normas establecidas, a las responsabilidades específicas del trabajo y al marco de habilidades y competencias. Los empleados deberían recibir preparación sobre aspectos de desempeño personal y conducta, siempre que sea apropiado.	APO07.03	Plan de formación en seguridad de la información	Evaluaciones del personal sobre seguridad de la información	Interna
	MEA01.02	Métricas y objetivos de seguridad de la información, consensuados		
	Fuera del *ámbito de COBIT 5 para Seguridad de la Información*	Política de Recursos Humanos		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Incorporar criterios de seguridad de la información a los procesos de evaluación del personal.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio. Comprender y realizar un seguimiento de la demanda, actual y futura, de recursos humanos para el negocio y TI con responsabilidades sobre las TI corporativas. Identificar las carencias y proporcionar datos de entrada para los planes de aprovisionamiento; los planes de abastecimiento de procesos de contratación de personal para el negocio y para TI; y los propios procesos de contratación para el negocio y para TI.	APO02.06	Plan de seguridad de la información	• Plan de seguimiento del rendimiento de los recursos e indicadores • Plan de asignación de recursos	Interna
	Fuera del *ámbito de COBIT 5 para Seguridad de la Información*	• Requisitos de recursos de proceso • Asignaciones de presupuesto • Listados de personal • Habilidades del personal		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Gestionar la asignación de personal de seguridad de la información de acuerdo a las necesidades de negocio.				

APO07 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO07.06 Gestionar el personal contratado. Asegúrese de que los consultores y el personal contratado que apoyan a la empresa con sus capacidades de TI, conocen y cumplen las políticas de la organización así como los requisitos contractuales previamente acordados.	APO01.03	Políticas de seguridad de la información y afines	Acuerdos de no divulgación y otras políticas firmadas por terceras partes	Interna
	APO02.06	Plan de seguridad de la información		
	BAI02.01	Requisitos de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Obtener la aceptación formal del personal en relación a los requisitos y políticas de seguridad de la información.				

Para más información acerca de los catalizadores relacionados, por favor consulta:
- Apéndice E. Guía Detallada: Catalizador de Información, E.7. Material de Concienciación
- Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias

Página dejada en blanco intencionadamente

APO08 Gestionar las Relaciones	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso de COBIT 5 Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves.	
Declaración del Propósito del Proceso de COBIT 5 Crear mejores resultados, mayor confianza en la tecnología y conseguir un uso efectivo de los recursos.	
APO08 Metas y Métricas del Proceso específicas de Seguridad:	
Metas del Proceso específicas de Seguridad	**Métricas Relacionadas**
1. Se ha establecido una estructura de coordinación, comunicación y enlace entre la función de seguridad de la información y varios grupos de interés	• Porcentaje de representación de la seguridad de la información en los comités de negocio
2. Los grupos de interés reconocen la seguridad de la información como un catalizador del negocio	• Tasa de inclusión de las iniciativas de seguridad de la información en las propuestas de inversión

APO08 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad

Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO08.01 Entender las expectativas del negocio. Entender los problemas y objetivos actuales del negocio y sus expectativas para TI. Asegurar que los requisitos son entendidos, gestionados y comunicados, y su estado acordado y aprobado.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Metas y objetivos del negocio	Comprensión de los procesos de negocio de la empresa	APO08.02 APO08.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Entender el negocio y cómo la seguridad de la información lo habilita/afecta.				

Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO08.02 Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio. Identificar oportunidades potenciales para que TI sea catalizadora de un mejor rendimiento empresarial.	APO04.03	Tendencias emergentes en seguridad de la información identificadas	Innovaciones en Seguridad de la Información	APO08.03
	APO08.01	Comprensión de los procesos de negocio de la empresa		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Entender las tendencias y las nuevas tecnologías en seguridad de la información y cómo pueden ser aplicadas, de modo innovador, para mejorar el rendimiento de los procesos de negocio.				

Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO08.03 Gestionar las relaciones con el negocio. Gestionar la relación con los clientes (representantes del negocio). Asegurar que los roles y responsabilidades de la relación están definidos, asignados y que se facilita la comunicación.	APO08.01	Comprensión de los procesos de negocio de la empresa	Estrategia para lograr el compromiso de las partes interesadas	Interna
	APO08.02	Innovaciones en seguridad de la información		
	DSS02.02	Incidentes y peticiones de servicio de seguridad de la información, clasificados y priorizados		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Establecer un método para influir en los contactos clave en relación con seguridad de la información.				

APO08 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO08.04 Coordinar y comunicar. Trabajar con las partes interesadas y coordinar, de extremo a extremo, la entrega de los servicios de TI y las soluciones proporcionadas al negocio.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Plan de comunicación corporativo	Estrategia de comunicación de la seguridad de la información	Interna
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Establecer los canales de comunicación adecuados entre la función de seguridad de la información y el negocio.				
2. Establecer la presentación de informes y métricas sobre seguridad de la información de forma adecuadas.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO08.05 Proveer datos de entrada para la mejora continua de los servicios. Mejorar y evolucionar continuamente los servicios basados es TI y la entrega del servicio a la empresa, para alinearlos con unos cambiantes requisitos de empresa y tecnológicos.	APO02.02	Capacidades de seguridad de la información	Integración de la seguridad de la información en el proceso de mejora continua	Interna
	BAI02.01	Requisitos de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Incorporar los requisitos de seguridad de la información al proceso de mejora continua.				

Para obtener más información acerca de los catalizadores relacionados, por favor consulte
- Apéndice C. Guía Detallada: Catalizador de Estructuras Organizativas, C.5. Depositarios de la Información/Dueños del Negocio.

APO09 Gestionar los Acuerdos de Servicio	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso de COBIT 5 Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento.	
Declaración del Propósito del Proceso de COBIT 5 Asegurar que los servicios TI y los niveles de servicio cubren las necesidades presentes y futuras de la empresa.	

APO09 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	**Métricas Relacionadas**
1. Los acuerdos de nivel de servicio (ANS) tienen en cuenta los requisitos de seguridad de la información	• Porcentaje de acuerdos de servicio que incluyen metas de seguridad de la información.

APO09 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO09.01 Identificar servicios TI. Analizar los requisitos del negocio y el modo en que los servicios de TI y los niveles de servicio soportan los procesos de negocio. Discutir y acordar servicios potenciales y niveles de servicio con el negocio, y compararlos con el vigente portafolio de servicios para identificar servicios nuevos o modificados, u opciones de nivel de servicio.			Requisitos de seguridad de la información en los servicios de TI identificados	APO09.02
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Identificar los requisitos de seguridad de información de los servicios de TI identificados.				
2. Definir y verificar el portafolio de servicios de seguridad de la información.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO09.02 Catalogar servicios basados en TI. Definir y mantener uno o más catálogos de servicios para grupos destinatarios relevantes. Publicar y mantener los servicios TI activos en los catálogos.	APO09.01	Requisitos de seguridad de la información en los servicios de TI identificados.	Catálogo de servicios de seguridad de la información	Interna
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Publicar un catálogo de servicios de seguridad de la información.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO09.03 Definir y preparar acuerdos de servicio. Definir y preparar los acuerdos de servicio basándose en las opciones de los catálogos de servicio. Incluir acuerdos internos de nivel de operaciones.	BAI03.11	Servicios de seguridad de la Información.	Acuerdos de nivel de servicio (ANSs)	APO09.04 DSS05.02 DSS05.03
			Acuerdos de nivel de operaciones (OLAs)	DSS05.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Incluir requisitos de seguridad de la información en todos los ANSs.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO09.04 Supervisar e informar de los niveles de servicio. Supervisar los niveles de servicio, informar de las mejoras e identificar tendencias. Proporcionar información de gestión adecuada para ayudar a la gestión del rendimiento.	APO09.03	Acuerdos de nivel de servicio (ANSs)	Informes de rendimiento de nivel de servicio de seguridad de la información	APO09.05
	BAI03.11	Servicios de seguridad de la Información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Vigilar la eficacia de la seguridad de la información dentro de la supervisión del nivel de servicio				

APO09 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO09.05 Revisar acuerdos de servicio y contratos. Llevar a cabo revisiones periódicas de los acuerdos de servicio y revisarlos cuando sea necesario.	APO02.02	Capacidades de seguridad de la información.	Acuerdos de nivel de servicios (ANSs) actualizados	Interna
	APO02.06	Plan de seguridad de la información.		
	APO09.04	Informes de rendimiento de nivel de servicio de seguridad de la información.		
	BAI02.01	Requisitos de seguridad de la información.		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Revisar periódicamente los requisitos de seguridad de la información en función de la actualización de las necesidades de negocio.				

Para obtener más información acerca de los catalizadores relacionados, por favor consulte
- Apéndice E. Guía Detallada: Catalizador de Información, E.9. Cuadro de Mando de la Seguridad de la Información.
- Apéndice F. Guía Detallada: Catalizador de Servicios, Infraestructura y Aplicaciones.

APO10 Gestionar los Proveedores	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso de COBIT 5 Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.	
Declaración del Propósito del Proceso de COBIT 5 Minimizar el riesgo de proveedores que no rindan y asegurar precios competitivos.	

APO10 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	**Métricas Relacionadas**
1. Se evalúa periódicamente a los proveedores y los contratos; y se disponen planes adecuados de mitigación del riesgo.	• Porcentaje de proveedores que cumplen los requisitos acordados • Nº de brechas de seguridad de los sistemas de información causados por proveedores • Nº de eventos de seguridad de la información que llevan a incidentes • Frecuencia de incidentes de seguridad de la información con proveedores • Nº de revisiones independientes de seguridad de la información de los proveedores
2. Los proveedores reconocen la seguridad de la información como un importante catalizador de negocio.	• Porcentaje de contratos con proveedores que incluyen requisitos de seguridad de la información • Nº de incidentes de seguridad de la información relacionados con proveedores

APO10 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO10.01 Identificar y evaluar las relaciones y contratos con proveedores. Identificar proveedores y contratos asociados y categorizarlos por tipo, relevancia y criticidad. Establecer un criterio de evaluación de contratos y proveedores y evaluar la cartera general de proveedores y contratos actuales y alternativos.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Análisis de riesgos de proveedores	Catalogo de proveedores	APO10.04 APO10.05 BAI03.04
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Llevar a cabo las evaluaciones de riesgos de la información y definir el perfil de riesgo de la misma.				
2. Definir la relación y requisitos de los proveedores basándose en el perfil de riesgo de la información.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO10.02 Seleccionar proveedores. Seleccionar proveedores de acuerdo a prácticas justas y formales que aseguren la selección del que mejor se adapte a los requisitos. Los requisitos deberían estar optimizados con las aportaciones de nuevos proveedores potenciales.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No son necesarias guías específicas sobre seguridad de la información para esta práctica. Las actividades genéricas de COBIT 5 pueden ser utilizadas como guía adicional.				

APO10 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO10.03 Gestionar contratos y relaciones con proveedores. Formalizar y gestionar las relaciones con cada proveedor. Gestionar, mantener y supervisar los contratos y la entrega de servicios. Asegurar que los nuevos contratos o los cambios son conformes a las normas de la empresa, a las leyes y a las regulaciones. Gestionar los conflictos contractuales.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No son necesarias guías específicas sobre seguridad de la información para esta práctica. Las actividades genéricas de COBIT 5 pueden ser utilizadas como guía adicional.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO10.04 Gestionar el riesgo en el suministro. Identificar y gestionar los riesgos relacionados con la capacidad de los proveedores de proporcionar de manera continua una entrega del servicio segura, eficaz y eficiente.	APO10.01	Catálogo de proveedores	Valoración del riesgo del proveedor, actualizada	APO10.05
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Reevaluar, periódicamente, los perfiles de seguridad de los proveedores, a partir de los requisitos de seguridad de la información y de otros tipos.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO10.05 Supervisar el cumplimiento y el rendimiento del proveedor. Revisar periódicamente el rendimiento general de los proveedores, el cumplimiento con los requisitos contractuales y la relación calidad-precio, y tratar las incidencias identificadas.	APO10.01 APO10.04	Catálogo de proveedores Valoración del riesgo del proveedor, actualizada	Resultado de la revisión del cumplimiento del proveedor	Interna
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Supervisar si los proveedores garantizan una entrega del servicio segura, eficiente y eficaz.				

A más información de los catalizadores relacionados, por favor consultar:
- Apéndice C. Guía Detallada: Catalizador de Estructuras Organizativas, C.4. Comité de Gestión de Riesgo Empresarial
- Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias, G.3. Gestión de Riesgo de la Información

APO11 Gestionar la Calidad	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso de COBIT 5 Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.	
Declaración del Propósito del Proceso de COBIT 5 Asegurar la entrega consistente de soluciones y servicios que cumplan con los requisitos de la organización y que satisfagan las necesidades de las partes interesadas.	

APO11 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	**Métricas Relacionas**
1. Se han definido e implementado los requisitos de calidad operativos para los servicios de seguridad de la información.	• Porcentaje, basado en encuestas, de partes interesadas satisfechas con la calidad de los servicios de seguridad de la información • Número de servicios con un plan formal de seguridad de la información • Frecuencia de presentación de informes (semanal, mensual, trimestral, anual) • Medida en que la resolución de cuestiones de seguridad de la información (incidentes, vulnerabilidades, puntos de auditoría, etc.) queda realizada de forma oportuna • Porcentaje de personal de seguridad de la información con credenciales profesionales (CISM, CISSP, etc.) • Número de horas de formación profesional continua (CPE), u horas de asistencia a formación o a eventos del sector

APO11 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO11.01 Establecer un sistema de gestión de la calidad (SGC). Establecer y mantener un SGC que proporcione una aproximación a la gestión de la calidad de la información para la información, la tecnología y los procesos de negocio que sea continua, estandarizada, formal y que esté alineada con los requerimientos del negocio y con la gestión corporativa de la calidad.	APO01.06	Roles y responsabilidades de la seguridad de la información	Buenas prácticas y normas relevantes de seguridad de la información	APO11.02
	APO02.02	Capacidades de seguridad de la Información		
	APO02.06	Plan de seguridad de la información.		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Determinar buenas prácticas de seguridad de la información.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO11.02 Definir y gestionar normas, practicas y procedimientos de seguridad. Identificar y mantener requisitos, normas, procedimientos y prácticas para los procesos clave, a fin de guiar a la empresa hacia el cumplimiento del propósito del QMS común, consensuado. Esto debería estar en línea con los requisitos del marco de control de TI. Considerar la certificación para los procesos, unidades organizativas, productos o servicios clave.	APO11.01	Buenas prácticas y normas relevantes para seguridad de la información	Normas de calidad dirigidas a la seguridad de la información	APO11.03 BAI03.06
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Alinear las prácticas de seguridad de la información con el sistema de gestión de la calidad (SGC).				

APO11 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO11.03 Enfocar la gestión de la calidad en los clientes. Enfocar la gestión de la calidad en los clientes, mediante la determinación de sus necesidades y asegurar el alineamiento con las prácticas de gestión de la calidad.	APO11.02	Normas de calidad dirigidas a la seguridad de la información	Acuerdos de nivel de servicio consensuados y cláusulas contractuales, relativos a la calidad de la seguridad de la información, cuando sea pertinente	APO11.04
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Obtener el consenso del cliente sobre los requisitos de los acuerdos de nivel de servicio de seguridad de la información.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO11.04 Supervisar y hacer controles y revisiones de la calidad. Supervisar la calidad de procesos y servicios de forma permanente como se defina en el SGC. Definir, planificar y aplicar medidas para supervisar la satisfacción del cliente con la calidad, así como el valor que proporciona el SGC. La información recogida debería ser utilizada por los propietarios de los procesos para mejorar la calidad.	APO11.03	Acuerdos de nivel de servicio consensuados y cláusulas contractuales, relativos a la calidad de la seguridad de la información, cuando sea pertinente	Métricas de la calidad de la seguridad de la información implementadas en línea con las buenas prácticas	APO11.05
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir métricas de la calidad de la seguridad de la información para medir la consecución de los requisitos de seguridad de la información y el funcionamiento eficiente de los controles de seguridad de la información.				
2. Supervisar las métricas de la calidad de la seguridad de la información.				
3. Adoptar acciones correctivas para subsanar problemas de calidad en la función de seguridad de la información.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO11.05 Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios. Incorporar prácticas pertinentes de gestión de la calidad en la definición, supervisión, notificación y gestión continua de los desarrollos de soluciones y los servicios ofrecidos.	APO11.04	Métricas de la calidad de la seguridad de la información implantadas en línea con las buenas prácticas	Enlace con el proceso de comunicación de incidentes de seguridad	Interna
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Identificar, documentar y comunicar el origen de los problemas con las métricas de calidad de la seguridad de la información.				
2. Aplicar prácticas correctivas para solucionar los problemas de calidad.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO11.06 Mantener una mejora continua. Mantener y comunicar regularmente un plan de la calidad global que promueva la mejora continua. Éste debería incluir la necesidad y los beneficios de una mejora continua. Recoger y analizar datos sobre el SGC y mejorar su eficacia. Corregir las no conformidades para prevenir la recurrencia. Promover una cultura mejora continua de la calidad.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No son necesarias guías específicas sobre seguridad de la información para esta práctica. Las actividades genéricas de COBIT 5 pueden ser utilizadas como guía adicional.				

APO12 Gestionar el Riesgo	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso de COBIT 5 Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.	
Declaración del Propósito del Proceso de COBIT 5 Integrar la gestión de riesgos empresariales relacionados con TI en la gestión general de riesgos corporativos (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI.	

APO12 Metas y Métricas del Proceso específicas de Seguridad	
Metas del Proceso específicas de Seguridad	**Métricas Relacionadas**
1. Se dispone de un perfil de riesgo, completo y vigente, para la tecnología, las aplicaciones y la infraestructura, dentro de la empresa.	• Existencia, vigencia y completitud de los perfiles de riesgo.
2. La respuesta a incidentes de seguridad de la información forma parte del proceso global de gestión del riesgo para proporcionar la capacidad de actualizar el portafolio de gestión del riesgo.	• Número de incidentes con valoraciones de riesgo adecuadamente diseñadas

APO12 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad

Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO12.01 Recopilar datos. Identificar y recopilar datos relevantes para hacer posible una identificación, análisis y notificación efectiva de riesgos relacionados con TI.	APO01.03	Políticas de seguridad de la información y afines	Datos sobre el riesgo de seguridad de la información	APO12.02 APO12.03
	APO01.08	Evaluación del cumplimiento de seguridad de la información		
	DSS02.02	Incidentes de seguridad de la información y solicitudes de servicio, clasificados y priorizados		
Actividades especificas de Seguridad (Adicionales a las actividades de COBIT 5)				
1. Identificar y recopilar datos relevantes para hacer posible una eficaz identificación, análisis y entrega de informes relativos a seguridad de la información.				

Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO12.02 Analizar el riesgo. Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tengan en cuenta la relevancia para el negocio de los factores de riesgo.	APO12.01	Datos sobre el riesgo de seguridad de la información	Resultados del análisis de seguridad de la información	APO12.03
	DSS05.01	Evaluación de las amenazas potenciales	Escenarios de riesgos de seguridad de la información	APO12.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Identificar, analizar y evaluar el riesgo de la información.				

Práctica de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	Desde	**Descripción**	**Descripción**	**Hacia**
APO12.03 Mantener un perfil de riesgo. Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados	EDM01.01	Principios que rigen la seguridad de la información	Perfil de riesgo de seguridad de la información	APO12.04 APO12.05 BAI01.01 BAI01.11 BAI02.03
	APO12.01	Datos sobre el riesgo de seguridad de la información		
	APO12.02	• Resultado del análisis de riesgo de seguridad de la información • Escenarios de riesgos de seguridad de la información		
	DSS05.01	Evaluación de potenciales amenazas		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Crear un perfil de riesgo que incluya aspectos de seguridad de la información.				

APO12 Prácticas, Entradas/Salidas y Actividades del Proceso específicas de Seguridad *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO12.04 Expresar el riesgo. Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de forma oportuna a todas las partes interesadas para una respuesta apropiada.	APO12.03	Perfil de riesgo de seguridad de la información	Estrategias de respuesta a riesgos de seguridad de la información	Interna
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir y poner en marcha la evaluación de riesgo y las estrategias de respuesta.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO12.05 Definir un portafolio de acciones para la gestión de riesgos. Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.	APO12.03	Perfil de riesgo de seguridad de la información	Propuestas de proyectos para reducir el riesgo de seguridad de la información	APO12.06
			Propuestas de proyectos para reducir el riesgo	APO13.02
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Supervisar continuamente los niveles de riesgo de las TI y de la información.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO12.06 Responder al riesgo. Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.	APO12.05	Propuestas de proyecto para reducir el riesgo de la seguridad de la información	Prácticas de reducción del riesgo de la seguridad de la información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Aplicar las prácticas seleccionadas de mitigación de riesgos de la seguridad de la información.				

Para más información de los catalizadores relacionados, por favor consultar:
- Apéndice C. Guía Detallada: Catalizador de Estructuras Organizativas, C.4. Comité de Gestión de Riesgo Empresarial
- Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias, G.3. Gestión de Riesgo de la Información

APO13 Gestionar de la Seguridad	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción Proceso COBIT 5 Definir, administrar y supervisar un sistema de gestión de seguridad de la información.	
Declaración del Propósito del Proceso COBIT 5 Mantener el impacto y la ocurrencia de incidentes de seguridad de la información dentro de los niveles de apetito al riesgo de la empresa.	

APO13 Objetivos y Métricas de Proceso específicos de seguridad	
Objetivos de Proceso específicos de Seguridad	**Métricas Relacionadas**
1. Está en marcha un sistema que considera y trata efectivamente los requerimientos de seguridad de la información de la empresa.	• Número de roles de seguridad claves claramente definidos • Número de incidentes relacionados con la seguridad
2. Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad.	• Nivel de satisfacción de las partes interesadas con el plan de seguridad en toda la empresa • Número de soluciones de seguridad que se desvían del plan • Número de soluciones de seguridad que se desvían de la arquitectura de empresa
3. Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la empresa.	• Número de servicios con alineamiento confirmado al plan de seguridad • Número de incidentes de seguridad causados por la no observancia del plan de seguridad • Número de soluciones desarrolladas con alineamiento confirmado al plan de seguridad

APO13 – Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO13.01 Establecer y mantener un SGSI. Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineado con los requerimientos de negocio y la gestión de seguridad en la empresa.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Enfoque de seguridad de la empresa	Declaración de alcance del SGSI	APO01.02 DSS06.03
			Política de SGSI	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir el alcance y los límites del SGSI en términos de las características de la empresa, la organización, su localización, activos y tecnología. Incluir detalles de y justificación para, cualquier exclusión del alcance.				
2. Definir un SGSI de acuerdo con la política de empresa y alineado con la empresa, la organización, su localización, activos y tecnología.				
3. Alinear el SGSI con el enfoque global de gestión de la seguridad en la empresa.				
4. Obtener autorización de la dirección para implementar y operar o cambiar el SGSI.				
5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.				
6. Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.				
7. Comunicar el enfoque del SGSI.				

APO13 – Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información. Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio.	APO02.04	Diferencias y cambios necesarios para alcanzar la capacidad objetivo	Casos de negocio de seguridad de la información	APO02.05
	APO03.02	Descripciones de dominios de partida y definición de arquitectura		
	APO12.05	Propuestas de proyectos para reducir el riesgo		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa. Asegurar que el plan identifica las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los riegos de seguridad de información identificados.				
2. Mantener un inventario de componentes de la solución implementados para gestionar los riesgos relacionados con la seguridad como parte de la arquitectura de la empresa.				
3. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, sustentados en casos de negocio adecuados que incluyan la consideración de la financiación y la asignación de roles y responsabilidades.				
4. Proporcionar información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas sobre la base del plan de tratamiento de riesgos de seguridad de la información.				
5. Definir la forma de medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizar estas mediciones para evaluar la efectividad y producir resultados reproducibles y comparables.				
6. Recomendar programas de formación y concienciación en seguridad de la información.				
7. Integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de seguridad de información y otros controles que permitan la prevención y detección temprana de eventos de seguridad, así como la respuesta a incidentes de seguridad.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**Desde**	**Descripción**	**Descripción**	**Hacia**
APO13.03 Supervisar y revisar el SGSI. Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua.	DSS02.02	Incidentes y requerimientos de servicios clasificados y priorizados	Recomendaciones para mejorar el SGSI	Interno
			Informes de auditoría del SGSI	MEA02.01
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Realizar revisiones periódicas del SGSI, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del SGSI. Considerar los resultados de auditorías de seguridad, incidentes, resultados de mediciones de efectividad, sugerencias y retroalimentación de todas las partes interesadas.				
2. Realizar auditorías internas al SGSI a intervalos planificados.				
3. Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se identifican mejoras en el proceso del SGSI.				
4. Proporcionar información para el mantenimiento de los planes de seguridad para que se incluyan las incidencias de las actividades de supervisión y revisión periódica.				
5. Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.				

B.3 Construir, Adquirir e Implementar (BAI)

01 Gestionar los programas y proyectos.

02 Gestionar la definición de requisitos.

03 Gestionar la identificación y construcción de soluciones.

04 Gestionar la disponibilidad y la capacidad.

05 Gestionar la introducción de cambios organizativos.

06 Gestionar los cambios.

07 Gestionar la aceptación del cambio y de la transición.

08 Gestionar el conocimiento.

09 Gestionar los activos.

10 Gestionar la configuración.

Página dejada en blanco intencionadamente

BAI01 Gestionar Programas y Proyectos	Área: Gestión Dominio: Construir, Adquirir e Implementar
Descripción Proceso COBIT 5 Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.	
Declaración del Propósito del Proceso COBIT 5 Alcanzar los beneficios de negocio y reducir el riesgo de retrasos y costes inesperados y el deterioro del valor, mediante la mejora de las comunicaciones y la involucración de usuarios finales y de negocio, asegurando el valor y la calidad de los entregables del proyecto y maximizando su contribución al portafolio de servicios e inversiones.	

BAI01 Objetivos y Métricas de Proceso específicos de seguridad	
Objetivos de Proceso específicos de Seguridad	**Métricas Relacionadas**
1. Se consideran y se incorporan los requisitos de seguridad de la información en todos los programas y proyectos.	• Porcentaje de programas y grupos de interés del proyecto comprometidos de manera efectiva en la gestión de Seguridad de la Información • Porcentaje de programas y proyectos que tienen un análisis de riesgos de seguridad y un plan de seguridad de la información para tratar el riesgo • Porcentaje de expertos en temas de seguridad de la información involucrados en los proyectos • Porcentaje de aprobaciones formales por parte de los grupos de interés de las etapas de revisión y planes de remediación • Frecuencia de las revisiones del estado de seguridad de la información • Grado de satisfacción de los grupos de interés con los aspectos de seguridad de la información en el proyecto en la revisión de cierre de proyecto

BAI01 – Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI01.01 Mantener un enfoque estándar para la gestión de programas y proyectos. Mantener un enfoque estándar para la gestión de programas y proyectos que posibilite revisiones y tomas de decisión de gobierno y de gestión y actividades de gestión de la entrega, enfocadas en la consecución de valor y de objetivos (requisitos, riesgos, costes, cronograma y calidad) para el negocio de una forma consistente.	AP001.03	Políticas de seguridad de la información y afines	Requisitos de seguridad de la información en el estudio de viabilidad	BAI01.02 BAI02.02 BAI03.01
	AP002.02	Capacidades de seguridad de la información		
	AP002.06	Plan seguridad de la información		
	AP012.03	Perfil de riesgo de seguridad de la información		
	BAI02.01	Requerimientos de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Incorporar los requerimientos de seguridad de la información en el estudio de viabilidad para cada proyecto dentro de los programas.				
2. Establecer un proceso para asegurar que se protege toda la información que se recoge o se produce como parte del proyecto.				

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI01.02 Iniciar un programa. Iniciar un programa para confirmar los beneficios esperados y para obtener la autorización para proceder. Esto incluye los acuerdos sobre el patrocinio del programa, confirmar el mandato del programa a través de la aprobación del caso de negocio conceptual, designar a los consejeros o los miembros del comité del programa, generar el expediente del programa, revisar y actualizar el caso de negocio, desarrollar un plan de realización de beneficios y obtener la aprobación de los patrocinadores para empezar.	BAI01.01	Requisitos de seguridad de la información en el estudio de viabilidad	Caso de negocio conceptual del programa que incluye las actividades obligatorias de seguridad de la información	BAI01.04 BAI01.08
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Planificar las actividades de seguridad de la información para cada proyecto dentro del programa general.				

BAI01 – Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI001.03 Gestionar el compromiso de las partes interesadas. Gestionar el compromiso de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna, que llegue a todos las partes interesadas relevantes. Esto incluye la planificación, identificación y el compromiso de las partes interesadas y la gestión de sus expectativas.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI01.04 Desarrollar y mantener el plan de programa. Formular un programa para definir las bases iniciales y posicionarlo para una ejecución exitosa mediante la formalización del alcance del trabajo a ser efectuado e identificando los entregables que satisfarán sus objetivos y la entrega de valor. Mantener y actualizar el plan del programa y el caso de negocio a lo largo del ciclo de vida económico completo del programa, asegurando el alineamiento con los objetivos estratégicos y reflejando el estado actual y los conocimientos obtenidos hasta el momento.	APO02.06	Plan de seguridad de la información	Plan conceptual del programa incluyendo las actividades obligatorias de seguridad de la información	BAI01.08
	BAI01.02	Caso de negocio conceptual del programa que incluye las actividades obligatorias de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Desarrollar un plan de seguridad de la información que identifique el entorno y los controles de seguridad de la información que el equipo del proyecto ha de implantar para proteger los activos organizativos.				
2. Incluir los recursos necesarios en los proyectos para identificar e implementar de forma efectiva los requerimientos de seguridad de la información.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI01.05 Lanzar y ejecutar el programa. Lanzar y ejecutar el programa para adquirir y dirigir los recursos necesarios para lograr las metas y beneficios definidos en el plan del programa. De acuerdo con los criterios de revisión de lanzamiento o cambio de fase (*stage-gate*), preparar los cambios de fase, las revisiones de las iteraciones o versiones para informar del progreso del programa y ser capaz de establecer los fundamentos para la financiación de la siguiente etapa después de la revisión del lanzamiento o de cambio de fase (*stage-gate*).				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI01.06 Supervisar, controlar e informar de los resultados del programa. Supervisar y controlar el rendimiento del programa (entrega de soluciones) y de la organización (valor/resultado) versus el plan durante el ciclo de vida económico completo de la inversión. Informar del rendimiento al comité estratégico del programa y a los patrocinadores.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

BAI01 – Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI01.07. Lanzar e iniciar proyectos dentro de un programa. Definir y documentar la naturaleza y el alcance del proyecto para confirmar y desarrollar entre las partes interesadas un entendimiento común del alcance del proyecto y cómo este se relaciona con otros proyectos dentro del programa general de inversiones de TI. La definición debería estar formalmente aprobada por el patrocinador del programa y del proyecto.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI01.08.Planificar Proyectos. Establecer y mantener un plan de proyecto formal, aprobado e integrado (que cubra los recursos del negocio y de TI) para guiar la ejecución del proyecto y controlarlo durante toda su vida. El alcance de los proyectos debería estar claramente definido y vinculado claramente a la construcción o aumento de la capacidad del negocio.	APO02.06	Plan de seguridad de la información	Plan de proyecto incluyendo las metas, objetivos y requerimientos de seguridad de la información	BAI01.10
	BAI01.02	Caso de negocio conceptual del programa incluyendo las actividades obligatorias de seguridad de la información		
	BAI01.04	Plan conceptual del programa incluyendo las actividades obligatorias de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Integrar la seguridad de la información en la gestión de proyectos de TI y de negocio				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI01.09 Gestionar la calidad de los programas y proyectos. Preparar y ejecutar un plan y procesos y prácticas de gestión de la calidad, alineadas con el SGC que describa el enfoque de calidad del programa y del proyecto y cómo será implementado. El plan debería ser formalmente revisado y acordado por todas las partes afectadas y, después, incorporado a los planes integrados del programa y los proyectos.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI01.10 Gestionar el riesgo de los programas y proyectos. Eliminar o minimizar los riesgos específicos asociados con los programas y proyectos mediante un proceso sistemático de planificación, identificación, análisis, respuesta, supervisión y control de las áreas o eventos que tienen el potencial de causar cambios no deseados. Los riesgos enfrentados por la administración del programa y los proyectos deberían ser establecidos y registrados en un único punto.	BAI01.08	Plan de proyecto incluyendo las metas, objetivos y requerimientos de seguridad de la información	Registro de riesgos de seguridad de la información incluido como parte del registro general de riesgos del proyecto	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Establecer un registro de riesgos de información y acciones correctivas para los riesgos identificados. Actualizar y revisar periódicamente el registro de riesgos.				
2. Integrar los proyectos de seguridad de la información en el proceso de gestión de programas y proyectos de la empresa.				

BAI01 – Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI01.11 Supervisar y controlar proyectos. Medir el desempeño del proyecto versus los criterios clave de rendimiento del proyecto, tales como la planificación, la calidad, el coste y el riesgo. Evaluar el impacto de las desviaciones en el proyecto y el programa general e informar los resultados a las partes interesadas clave.	APO01.03	Políticas de seguridad de la información y afines	Informe de evaluación de proyectos de seguridad de la información identificando las debilidades de control y los planes de acciones correctivas recomendadas	Interno
	APO02.06	Plan de seguridad de la información		
	APO12.03	Perfil de riesgo de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Realizar evaluaciones periódicas independientes de los proyectos para asegurar que los requisitos de seguridad de la información son implementados efectivamente.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI01.12 Gestionar los recursos y los paquetes de trabajo del proyecto. Gestionar los paquetes de trabajo del proyecto mediante requerimientos formales de autorización y aceptación de los paquetes de trabajo, y asignando y coordinando los recursos de negocio y de TI adecuados.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI01.13 Cerrar un proyecto o iteración. Solicitar a las partes interesadas del proyecto, al final de cada proyecto, versión o iteración, que evalúen si el proyecto, la versión o la iteración entregaron los resultados y valor planeados. Identificar y comunicar cualquier actividad pendiente necesaria para lograr los resultados del proyecto y los beneficios del programa planeados, identificar y documentar las lecciones aprendidas para utilizar en futuros proyectos, versiones, iteraciones y programas.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI01.14 Cerrar un programa. Eliminar el programa del portafolio de inversiones activas cuando haya acuerdo de que el valor deseado ha sido logrado o cuando esté claro que no será logrado con los criterios de valor establecidos para el programa.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

Para más información respecto a los catalizadores relacionados, por favor consultar:
- Apéndice E. Guía Detallada: Catalizador de Información, E.4. Plan de Seguridad de la Información, E.6. Requisitos de Seguridad de la Información.
- Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias, G.3. Gestión de Riesgos de la Información.

BAI02 Gestionar la Definición de Requisitos	Área: Gestión Dominio: Construir, Adquirir e Implementar
Descripción del Proceso COBIT 5 Identificar soluciones y analizar requisitos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocio, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes y beneficios relacionados, análisis de riesgo y aprobación de los requisitos y soluciones propuestas.	
Declaración del Propósito del Proceso COBIT 5 Crear soluciones viables y óptimas que cumplan con las necesidades de la organización mientras minimizan el riesgo.	

BAI02 Objetivos y Métricas de Proceso específicos de seguridad	
Objetivos de Proceso específicos de Seguridad	**Métricas Relacionadas**
1. Se ha identificado e implementado todos los aspectos de seguridad de la información relevantes como requisitos técnicos y funcionales.	• Porcentaje de nuevos requerimientos de seguridad de la información añadidos por requerimiento del negocio • Porcentaje de requerimientos redefinidos debido a los requerimientos de seguridad de la información
2. Se ha detectado y añadido el riesgo de información asociado con requisitos técnicos y funcionales de negocio.	• Nuevos riesgos de seguridad de la información identificados. • Número de incidentes de seguridad de la información que indiquen riesgos nuevos o desconocidos • Número de incidentes de seguridad de la información basados en riesgos conocidos

BAI02 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
BAI02.1 Definir y mantener los requisitos técnicos y funcionales de negocio. Based on the business case, identify, prioritise, specify and agree on business information, functional, technical and control requirements covering the scope/understanding of all initiatives required to achieve the expected outcomes of the proposed IT-enabled business solution.	APO01.03	Políticas de seguridad de la información y afines	Requerimientos de seguridad de la información	APO02.03 APO04.04 APO07.06 APO08.05 APO09.05 BAI01.01 BAI02.04 BAI03.01 BAI03.04 BAI03.07 BAI03.09 BAI04.03 BAI05.01 MEA01.01 MEA03.01
	APO02.02	Capacidades de seguridad de la información		
	APO02.06	Plan de seguridad de la información		
	MEA03.01	Requerimientos externos de cumplimiento de seguridad de la información		

Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)

1. Investigar, definir y documentar los requisitos de seguridad de la información p.ej. requisitos de confidencialidad, integridad y disponibilidad.
2. Investigar y analizar los requisitos de seguridad de la información con las partes interesadas, patrocinadores de negocio y personal de implementación técnica.
3. Asegurar que los requisitos de negocio tienen en cuenta las necesidades de protección de seguridad de la información.

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
BAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas. Realizar un estudio de viabilidad de las potenciales soluciones alternativas, evaluando su viabilidad y seleccionando la opción preferida. Si se considera, implementar la opción seleccionada como un piloto para determinar posibles mejoras.	BAI01.01	Requerimientos de seguridad de la información en el estudio de viabilidad	Resultados del estudio de viabilidad	Interno

Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)

1. Asegurar que los requisitos de seguridad de la información son incluidos en el estudio de viabilidad

BAI02 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI02.03 Gestionar los riesgos de los requerimientos. Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos al procesamiento de la información y asociados con los requerimientos de la empresa y solución propuesta.	APO12.03	Perfil de riesgo de seguridad de la información	Acciones de mitigación del riesgo	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Realizar una evaluación de riesgos de la información para identificar los controles de seguridad de la información para las actividades relevantes del negocio (gestión del programa y proyectos incluidos).				
2. Cooperar con el responsable de riesgos para gestionar los riesgos de la información.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI02.04 Obtener la aprobación de los requerimientos y soluciones. Coordinar la realimentación de las partes interesadas afectadas y, en las fases clave predeterminadas, obtener la aprobación y la firma del patrocinador o propietario del producto y cierre de los requerimientos técnicos y funcionales, de los estudios de viabilidad, de los análisis de riesgos y de las soluciones recomendadas.	BAI02.01	Requerimientos de seguridad de la información	Aprobación de los requerimientos de seguridad de la información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Validar los requerimientos de seguridad de la información con las partes interesadas, patrocinadores de negocio y personal técnico de implementación.				

Para más información respecto al catalizador relacionado, por favor consultar:
- Apéndice E. Guía Detallada: Catalizador de Información, E.6. Requisitos de Seguridad de la Información.
- Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias, G.3. Gestión de Riesgos de la Información.

BAI03 Gestionar la Identificación y Construcción de Soluciones	Área: Gestión Dominio: Construir, Adquirir e Implementar
Descripción del Proceso COBIT 5 Establecer y mantener soluciones identificadas en línea con los requisitos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.	
Declaración del Propósito del Proceso COBIT 5 Establecer soluciones puntuales y rentables capaces de soportar los objetivos estratégicos y operativos de la empresa.	

BAI03 Objetivos y Métricas de Proceso específicos de seguridad	
Objetivos de Proceso específicos de seguridad	**Métricas Relacionadas**
1. Las métricas de seguridad de la información se incorporan en la solución y apoyan de manera eficaz la estrategia de negocio y los objetivos operacionales.	• Número de diseños de la solución añadidos debido a los requerimientos de seguridad de la información • Número de excepciones de seguridad en el diseño y en la implementación
2. Las soluciones en seguridad de la información se aceptan y se han probado de manera satisfactoria.	• Número de pruebas adicionales para la seguridad de la información
3. Los cambios en los requerimientos de seguridad de la información se incorporan correctamente a la solución.	• Número de cambios aprobados relativos a requerimientos de seguridad de la información

BAI03 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
BAI03.01 Diseñar soluciones de alto nivel. Desarrollar y documentar diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas. Asegurar el alineamiento con la estrategia TI y la arquitectura empresarial. Revalorar y actualizar los diseños cuando sucedan cuestiones significativas durante las fases de diseño detallado o de construcción o según la solución evolucione. Asegurar que las partes interesadas participen activamente en el diseño y en la aprobación de cada versión.	BAI01.01	Requerimientos de seguridad en el estudio de viabilidad	Especificaciones de seguridad de la información en línea con los diseños de alto nivel	BAI03.02
	BAI02.01	Requerimientos de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir las especificaciones de seguridad de la información en línea con el diseño de alto nivel.				

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
BAI03.02 Diseñar los componentes detallados de la solución. Desarrollar, documentar y elaborar diseños detallados progresivamente usando técnicas de desarrollo ágiles o por fases acordadas previamente considerando todos los componentes (procesos de negocio y controles automáticos o manuales relacionados, aplicaciones soporte de TI, servicios de infraestructura y productos tecnológicos y proveedores/fabricantes). Asegurar que el diseño detallado incluye ANSs y OLAs internos Y externos.	BAI03.01	Especificaciones de seguridad de la información en línea con los diseños de alto nivel	Diseño de la seguridad de la información en los componentes de la solución	BAI03.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Integrar el diseño de la seguridad de la información en los componentes de la solución.				

BAI03 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI03.03 Desarrollar los componentes de la solución. Desarrollar los componentes de la solución progresivamente conforme el diseño detallado siguiendo los métodos de desarrollo, estándares de documentación, requerimientos de calidad (QA) y estándares de aprobación. Asegurar que se consideran todos los requerimientos de control en los procesos de negocio, soportando las aplicaciones TI y servicios de infraestructura, productos tecnológicos y servicios y proveedores/suministradores.	BAI03.02	Diseño de la seguridad de la información en los componentes de la solución	Prácticas de programación y bibliotecas de infraestructura seguras	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Verificar que todos los componentes de la solución incorporan prácticas de programación y bibliotecas de infraestructura seguras.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI03.04 Obtener los componentes de la solución. Obtener los componentes de la solución sobre la base del plan de adquisiciones y conforme a los requerimientos y diseños detallados, principios de arquitectura y estándares y en los procedimientos generales contractuales y de adquisiciones de la empresa, requerimientos de calidad (QA) y estándares de aprobación. Asegurar que todos los requerimientos legales y contractuales son identificados y cumplidos por el proveedor .	APO10.01	Catálogo de proveedores	Requerimientos de seguridad de la información dentro del plan de adquisiciones	Interno
	BAI02.01	Requerimientos de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que los requerimientos de seguridad forman parte del plan de adquisiciones y que se han realizado unas evaluaciones de seguridad de la información apropiadas.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI03.05 Construir soluciones. Instalar y configurar las soluciones e integrarlas con las actividades de los procesos de negocio. Implementar controles, medidas de seguridad y "auditabilidad" durante la configuración y durante la integración del hardware e infraestructura del el software para proteger los recursos y asegurar la disponibilidad e integridad de los datos. Actualizar el catálogo de servicios para reflejar la nueva situación.			Soluciones seguras	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Verificar que los aspectos de la seguridad de la información están incluidos en la construcción de la solución.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI03.06 Realizar controles de calidad. Desarrollar y ejecutar un plan de calidad (QA) alineado con el SGC para obtener la calidad especificada en la definición de los requerimientos y de acuerdo a las políticas y procedimientos de calidad de la empresa.	APO11.02	Estándares de calidad para la seguridad de la información	Resultados, excepciones y correcciones de la revisión de la calidad de la seguridad de información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Verificar que los aspectos de la seguridad de la información están incluidos en el aseguramiento de la calidad.				

BAI03 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI03.07 Preparar pruebas de la solución. Establecer un plan de pruebas y entornos necesarios para probar los componentes individuales y de la solución integrada, incluyendo los procesos de negocio y servicios, aplicaciones e infraestructura que los soportan.	BAI02.01	Requerimientos de seguridad de la información	Casos de prueba de la seguridad de la información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Incluir los casos de prueba de seguridad de la información en los planes de pruebas.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI03.08 Ejecutar pruebas de la solución. Ejecutar pruebas continuamente durante el desarrollo, incluyendo pruebas de control, en concordancia con el plan de pruebas y con las prácticas de desarrollo en el entorno apropiado. Hacer partícipes a los dueños de los procesos de negocio y usuarios finales en el equipo de pruebas. Identificar, registrar y priorizar los errores e incidentes identificados durante las pruebas.	APO01.03	Políticas de seguridad de la información y afines	Informe de aceptación de la seguridad	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Garantizar la seguridad de la información de todos los datos de producción usados en los casos de prueba, incluyendo la utilización de un proceso seguro para desnaturalizar los datos sensibles antes de su uso.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI03.09 Gestionar cambios a los requerimientos. Hacer seguimiento del estado de los requerimientos individuales (incluyendo todos los requerimientos rechazados) a través de todo el ciclo de vida del proyecto y gestionar la aprobación de los cambios a los requerimientos.	BAI02.01	Requerimientos de seguridad de la información	Registro de todas las peticiones de cambios aprobadas y aplicadas	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Gestionar los cambios en los aspectos y requerimientos de la seguridad de la información.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI03.10 Mantener soluciones. Desarrollar y ejecutar un plan para el mantenimiento de la solución y componentes de la infraestructura. Incluir revisiones periódicas respecto a las necesidades del negocio y requerimientos operacionales.			Soluciones seguras actualizadas	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que las actualizaciones de los requerimientos de seguridad de la información se reflejan en las actualizaciones de mantenimiento de las soluciones.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI03.11 Definir los servicios de TI y mantener el catálogo de servicios. Definir y acordar nuevos servicios TI o cambios y opciones de nivel de servicio. Documentar nuevas definiciones o cambios en los servicios y opciones de nivel de servicio que serán actualizadas en el catálogo de servicios.	Modelo de catalizadores de estructuras organizativas	Roles y responsabilidades	Servicios de seguridad de la información	APO09.03 APO09.04
	Fuera *de COBIT 5 para Seguridad de la Información*	• Misión/Visión de negocio • Metas y objetivos de negocio		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir los servicios de seguridad de la información en concordancia con las necesidades de negocio y las necesidades de cumplimiento o normativas.				
2. Definir los procesos de seguridad de la información dentro de los servicios de TI.				

Para más información relativa a los catalizadores, por favor consultar:
• Apéndice F. Guía Detallada: Catalizador de Servicios, Infraestructura y Aplicaciones.

Página dejada en blanco intencionadamente

BAI04 Gestionar la Disponibilidad y la Capacidad	Área: Gestión Dominio: Construir, Adquirir e Implementar
Descripción del Proceso COBIT 5 Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en coste. Incluir la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos de negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados.	
COBIT 5 Process Purpose Statement Mantener la disponibilidad del servicio, la gestión eficiente de recursos y la optimización del rendimiento de los sistemas mediante la predicción del rendimiento futuro y de los requerimientos de capacidad.	

BAI04 Objetivos y Métricas de Proceso específicos de seguridad	
Objetivos de Proceso específicos de seguridad	**Métricas Relacionadas**
1. Los requerimientos de seguridad de la información se incluyen en los planes de disponibilidad, rendimiento y gestión de la capacidad.	• Porcentaje de compromisos de seguridad de la información alcanzados.
2. Se monitoriza y optimiza el impacto de la seguridad de la información sobre la disponibilidad, el rendimiento y la capacidad.	• Porcentaje de incidentes de disponibilidad, rendimiento y capacidad por año causados por los controles de seguridad de la información.

BAI04 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia. Evaluar la disponibilidad, el rendimiento y la capacidad de los servicios y recursos para asegurar que se encuentra disponible una capacidad y un rendimiento justificables en costes para dar soporte a las necesidades del negocio y para entregar el servicio de acuerdo a los ANSs. Crear líneas de referencia para la disponibilidad, el rendimiento y la capacidad para comparaciones futuras.	APO02.02	Capacidades de seguridad de la información	Listado de problemas de seguridad de la información técnicos y procedimentales relativos a la disponibilidad, el rendimiento y la capacidad	BAI04.02
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Identificar los problemas de seguridad de la información técnicos y procedimentales relativos a la disponibilidad, el rendimiento y la capacidad..				

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI04.02 Evaluar el impacto en el negocio. Identificar los servicios importantes para la empresa, mapear los servicios y recursos con los procesos de negocio e identificar las dependencias de negocio. Asegurar que el impacto de la indisponibilidad de recursos está acordado y aceptado por el cliente. Asegurar que, para las funciones vitales del negocio, los requisitos de disponibilidad definidos en el ANS pueden ser satisfechos.	BAI04.01	Listado de problemas de seguridad de la información técnicos y procedimentales relativos a la disponibilidad, el rendimiento y la capacidad	Evaluaciones del impacto de la seguridad de la información sobre la disponibilidad, el rendimiento y la capacidad	BAI04.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Evaluar el impacto en la seguridad de la información de potenciales faltas de disponibilidad, pérdidas de rendimiento y faltas de capacidad en la seguridad de la información.				

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI04.03 Planificar para requisitos de servicios nuevos o modificados. Planificar y priorizar las implicaciones en la disponibilidad, el rendimiento y la capacidad de cambios en las necesidades del negocio y en los requerimientos de servicio.	BAI02.01	Requerimientos de seguridad de la información	Actualizaciones en los requerimientos de seguridad de la información	Interno
	BAI04.02	Evaluaciones del impacto de la seguridad de la información sobre la disponibilidad, el rendimiento y la capacidad		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Evaluar el impacto de requerimientos nuevos o modificados en la seguridad de la información.				

BAI04 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI04.04 Supervisar y revisar la disponibilidad y la capacidad. Supervisar, medir, analizar, informar y revisar la disponibilidad, el rendimiento y la capacidad. Identificar desviaciones respecto a la línea base establecida. Revisar informes de análisis de tendencias identificando cualquier cuestión y variación significativa, iniciando acciones donde sea necesario y asegurando que se realiza el seguimiento de todas las cuestiones pendientes.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI04.05 Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad. Abordar las desviaciones investigando y resolviendo las cuestiones identificadas relativas a disponibilidad, rendimiento y capacidad.			Actualizaciones de las acciones correctivas para resolver las cuestiones relativas a la capacidad	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Valorar e investigar cualquier cuestión relativa a la seguridad de la información que impacte en la disponibilidad, el rendimiento y la capacidad.				

BAI05 Gestionar la Introducción del Cambio Organizativo	Área: Gestión Dominio: Construir, Adquirir e Implementar
Descripción del Proceso COBIT 5 Maximizar la probabilidad de la implementación exitosa en toda la empresa del cambio organizativo de forma rápida y con riesgo reducido, cubriendo el ciclo de vida completo del cambio y a todas las partes interesadas del negocio y de TI.	
Declaración del Propósito del Proceso COBIT 5 Preparar y comprometer a las partes interesadas para el cambio en el negocio y reducir el riesgo de fracaso.	

BAI05 Objetivos y Métricas de Proceso específicos de seguridad	
Objetivos de Proceso específicos de seguridad	**Métricas Relacionadas**
1. Las alertas y tendencias en seguridad de la información son usadas de manera eficaz para facilitar el cambio en la organización e influir sobre la cultura corporativa en relación a la seguridad de la información.	• Nivel de implicación de la alta dirección en los programas y estrategias de seguridad de la información • Nivel de satisfacción de los actores que operan, utilizan y mantienen el cambio • Porcentaje de usuarios formados adecuadamente para los cambios en seguridad de la información como parte del cambio organizacional
2. Los protocolos relativos a la seguridad de la información se revisan y afinan como cambios corporativos a través de procesos de concienciación en el ámbito de la seguridad de la información.	• Nivel de satisfacción de los usuarios con la adopción del cambio

BAI05 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
BAI05.01 Establecer el deseo de cambiar. Comprender el alcance e impacto del cambio divisado y la disposición/voluntad de cambiar de las partes interesadas. Identificar las acciones para motivar a las partes interesadas para aceptar y querer que el cambio sea exitoso.	AP001.03	Políticas de seguridad de la información y afines	• Plan de comunicación con la alta dirección • Procesos de control del cambio acordados en línea con guías de buenas prácticas	Interno
	BAI02.01	Requerimientos de seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Establecer una cultura proactiva en seguridad de la información				
2. Identificar y comunicar los puntos críticos o débiles relativos a seguridad de la información y también los comportamientos deseables, incluyendo los cambios necesarios para abordar estos puntos.				
3. Proporcionar liderazgo visible a través del compromiso de la alta dirección (al más alto nivel, CxO) con la seguridad de la información para facilitar los cambios.				

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
BAI05.02 Formar un equipo de implementación efectivo. Establecer un equipo de implementación efectivo, con miembros adecuados, creando confianza y estableciendo metas comunes y medidas efectivas.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Habilidades personales	Equipos de implementación de seguridad de la información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Designar profesionales de la seguridad de la información cualificados para servir en los equipos de implementación.				
2. Desarrollar una visión común para todo el equipo de seguridad de la información.				

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
BAI05.03 Comunicar la visión deseada. Comunicar la visión deseada para el cambio en el lenguaje de aquellos que se verán afectados. La comunicación debería ser realizada por la alta dirección e incluir la razón de ser y los beneficios del cambio, el impacto de no hacerlo y la visión, la hoja de ruta y la participación requerida de las diversas partes interesadas.	AP002.06	Plan de seguridad de la información	Plan de comunicación de la visión referente a seguridad de la información	BAI05.04
	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Declaraciones corporativas de la visión/misión		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Comunicar la visión relativa a seguridad de la información como apoyo a la visión corporativa.				

BAI05 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI05.04 Facultar a los que juegan algún papel e identificar ganancias en el corto plazo. Facultar a aquellos con roles en la implementación asegurando que se han asignado las responsabilidades, se ha dado formación y se han alineado las estructuras organizativas y procesos de RRHH. Identificar y comunicar ganancias en el corto plazo que pueda ser realizadas y resulten importantes desde una perspectiva de posibilitar el cambio.	APO02.05	Hoja de ruta estratégica de seguridad de la información	Lista de los beneficios potenciales a corto plazo	BAI05.05
	APO02.06	Plan de seguridad de la información		
	BAI05.03	Plan de comunicación de la visión relativa a seguridad de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Alinear las prácticas de seguridad de la para apoyar la visión.				
2. Asignar de manera clara la responsabilidad de cada persona del equipo e incluir criterios de rendimiento para a establecer quiénes son los responsables de que se lleve a cabo el proceso.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI05.05 Facilitar la operación y el uso. Planificar e implementar todos los aspectos técnicos, operativos y de modo de uso de forma que todos aquellos involucrados en el entorno futuro puedan ejercer sus responsabilidades.	BAI05.04	Lista de los beneficios potenciales a corto plazo	Medidas prácticas de seguridad de la información	BAI05.06
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Desarrollar medidas prácticas de seguridad de la información.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI05.06 Integrar nuevos enfoques. Integrar nuevos enfoques mediante el seguimiento de los cambios implementados, asegurando la efectividad del plan de operación y uso y manteniendo un plan de concienciación mediante comunicaciones regulares. Aplicar las medidas correctoras que se estime apropiado y que podrían incluir el forzar el cumplimiento.	BAI05.05	Medidas prácticas de seguridad de la información	Prácticas operativas de seguridad de la información	Interno
Security-specific Activities (in Addition to COBIT 5 Activities)				
1. Hacer seguimiento continuo de la concienciación en seguridad de la información y adaptar pertinentemente las métricas.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI05.07 Mantener los cambios. Mantener los cambios mediante la formación eficaz del personal nuevo, campañas de comunicación periódicas, compromiso de la alta dirección, supervisión de la adopción de los cambios y divulgación a toda la empresa de las lecciones aprendidas.			Revisiones del uso operativo	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Informar y formar al nuevo personal y proporcionar sesiones de actualización de concienciación en seguridad de la información.				

Para más información respecto a los catalizadores referidos, por favor consultar:
- Apéndice D. Guía Detallada: Catalizador de Cultura, Ética y Comportamiento

BAI06 Gestionar los Cambios	Área: Gestión Dominio: Construir, Adquirir e Implementar
Descripción del Proceso COBIT 5 Gestione todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, informes, cierre y documentación.	
Declaración del Propósito del Proceso COBIT 5 Posibilitar una entrega de los cambios rápida y fiable para el negocio, al a vez que se mitiga cualquier riesgo que impacte negativamente en la estabilidad e integridad del entorno en que se aplica el cambio.	

BAI06 Objetivos y Métricas de Proceso específicas de seguridad	
Objetivos de Proceso específicos de seguridad	**Métricas Relacionadas**
1. Los requerimientos de seguridad de la información se incorporan durante la evaluación del impacto del cambio en los procesos, aplicaciones e infraestructuras.	• Número de cambios relevantes en cuanto a seguridad de la información y número de cambios que tengan impacto en la seguridad de la información. • Número de requerimientos de seguridad de la información que no se han cumplido después del cambio.
2. Los cambios de emergencia tienen en cuenta los requerimientos necesarios de seguridad de la información.	• Número de incidentes de seguridad de la información relativos a los cambios en el entorno. • Número de incidentes de seguridad de la información relativos a cambios en hardware y software.

BAI06 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio. Evaluar todas las peticiones de cambio para determinar su impacto en los procesos de negocio y los servicios TI, y analizar si el cambio afectará negativamente al entorno operativo e introducirá un riesgo inaceptable. Asegurar que los cambios son registrados, priorizados, categorizados, analizados, autorizados, planificados y programados.	APO01.03	Políticas de seguridad de la información y afines	Evaluaciones de impacto	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que se realiza una evaluación del impacto potencial de los cambios en seguridad de la información.				
2. Asegurar que la política de seguridad de la información se adapta a los objetivos de negocio de la empresa.				
3. Asegurar que los cambios están conformes con la política de seguridad de la información.				
4. Desarrollar prácticas que tengan en cuenta el impacto de nuevas tecnologías y tendencias en la seguridad de la información.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI06.02 Gestionar cambios de emergencia. Gestionar cuidadosamente los cambios de emergencia para minimizar futuras incidencias y asegurar que el cambio está controlado y se realiza de forma segura. Verificar que los cambios de emergencia son evaluados debidamente y autorizados de una vez hecho el cambio.			Revisión de seguridad de la información post-implementación de los cambios de emergencia	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Desarrollar medidas que contemplen los cambios de emergencia y mantenimiento sin comprometer la seguridad de la información.				
2. Para asegurar un seguimiento adecuado, mantener un registro de riesgos en la información cuando se introduzca un nuevo riesgo a raíz de un cambio de emergencia.				

BAI06 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI06.03 Hacer seguimiento e informar de cambios de estado. Mantener un sistema de seguimiento e informe que documente los cambios rechazados, comunique el estado de cambios aprobados y en proceso y de cambios completados. Asegurar que los cambios aprobados son implementados como esté previsto.			Informes actualizados del estado de las solicitudes de cambio	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Abordar las cuestiones de rendimiento y capacidad potenciales resultantes de los cambios propuestos en seguridad de la información.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI06.04 Cerrar y documentar los cambios. Siempre que el cambio haya sido implementado, actualizar, de manera consecuente, la documentación de la solución y del usuario, así como los procedimientos a los que afecta el cambio.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

Para más información respecto a los catalizadores relacionados, por favor consultar:
- Apéndice A. Guía Detallada: Catalizador de Principios, Políticas y Marcos de Trabajo
- Apéndice F. Guía Detallada: Catalizador de Servicios

BAI07 Gestionar la Aceptación del Cambio y la Transición	Área: Gestión Dominio: Construir, Adquirir e Implementar
Descripción del Proceso COBIT 5 Aceptar formalmente y hacer operativas las nuevas soluciones, incluyendo la planificación de la implementación, la conversión de los datos y los sistemas, las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de procesos de negocio o servicios TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación.	
Declaración de Propósito del Proceso COBIT 5 Implementar soluciones de forma segura y en línea con las expectativas y resultados acordados.	

BAI07 Objetivos y Métricas de Proceso específicos de Seguridad	
Objetivos de Proceso específicos de Seguridad	**Métricas Relacionadas**
1. Las pruebas de seguridad de la información son parte integral de las pruebas de aceptación.	• Número de cambios relacionados con la seguridad de la información que han sido rechazados o no han sido implementados • Porcentaje de cambios relacionados con la seguridad de la información aceptados
2. Las mejoras de seguridad de la información identificadas se incorporarán en futuros lanzamientos.	• Número de cuestiones abiertas de seguridad de la información por lanzamiento • Cambios en el número de cuestiones de seguridad de la información no resueltas por lanzamiento • Porcentaje de pruebas de seguridad de la información completadas en los cambios

BAI07 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI07.01 Establecer un plan de implementación. Establecer un plan de implementación que cubra la conversión de datos y sistemas, criterios de aceptación de las pruebas, comunicación, formación, preparación del lanzamiento, paso a producción, soporte inicial en producción, plan de marcha atrás o de contingencia y una revisión post-implantación. Obtener la aprobación de las partes relevantes.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Plan de Implementación TI	Plan de Implementación TI actualizado	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Incluir aspectos de seguridad de la información en la aceptación y en el plan de implementación de la transición.				

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI07.02 Planificar la conversión de procesos de negocio, sistemas y datos. Preparar la migración de procesos de negocio, datos de los servicios de TI e infraestructuras como parte de los mecanismos de desarrollo de la empresa, incluyendo registros de auditoría y un plan de recuperación para el caso de que la migración fallara.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI07.03 Planificar pruebas de aceptación. Establecer un plan de pruebas basado en estándares corporativos que defina roles, responsabilidades, y criterios de entrada y salida. Asegurar que el plan es aprobado por las partes relevantes.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Planes de prueba	Medidas de seguridad de la información en el entorno de prueba	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que las pruebas de aceptación de seguridad de la información son parte del plan de pruebas.				

BAI07 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI07.04 Establecer un entorno de pruebas. Definir y establecer un entorno seguro de pruebas que sea representativo del proceso de negocio y entorno de operaciones de TI planeados, en cuanto a rendimiento y capacidad, seguridad, controles internos, prácticas de operación, calidad de los datos y requisitos de privacidad y carga de trabajo.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Datos y arquitectura de entorno de pruebas	Entorno de pruebas seguro	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que existen los controles de seguridad de la información adecuados en el entorno de pruebas (p.ej. anonimato de los datos sensibles).				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI07.05 Ejecutar pruebas de aceptación. Probar los cambios independientemente, de acuerdo con el plan de pruebas definido, antes de migrar al entorno de producción.	Fuera de *COBIT 5 para Seguridad de la Información*	Pruebas de aceptación	Pruebas de aceptación actualizadas	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Desarrollar y ejecutar las pruebas de aceptación de seguridad de la información.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI07.06 Pasar a producción y gestionar los lanzamientos.. Pasar la solución aceptada al negocio y las operaciones. Donde sea apropiado, ejecutar la solución como un proyecto piloto o en paralelo con la solución antigua durante un período de tiempo definido y comparar su comportamiento y resultados. Si se dieran problemas significativos, reinstaurar el entorno original de acuerdo al plan de marcha atrás o alternativo. Gestionar los lanzamientos de los componentes de la solución.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Planes de lanzamiento	Planes de lanzamiento actualizados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que la seguridad de la información es gestionada durante el paso a producción y la gestión del lanzamiento.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI07.07 Proporcionar soporte en producción desde el primer momento. Proporcionar soporte desde el primer momento a los usuarios y a las operaciones de TI durante un periodo de tiempo acordado para tratar cualquier incidencia y ayudar a estabilizar la nueva solución.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI07.08 Ejecutar una revisión post-implantación. Llevar a cabo una revisión post-implantación para confirmar salidas y resultados, identificar lecciones aprendidas y desarrollar un plan de acción. Evaluar y verificar el rendimiento actual y las salidas del servicio nuevo o modificado respecto al rendimiento y salidas previstas (es decir, el servicio esperado por el usuario o el cliente).	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Informes de la revisión post-implementación	Informes de la revisión post-implementación actualizados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que la seguridad de la información se incluye en la revisión post-implementación.				

Para más información respecto de los catalizadores relacionados, por favor consultar:
- Apéndice F. Guía Detallada: Catalizador de Servicios, Infraestructura y Aplicaciones
- Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias; G.5 Operaciones de Seguridad de la Información

BAI08 Gestionar el Conocimiento	Área: Gestión Dominio: Construir, Adquirir e Implementar
Descripción del Proceso COBIT 5 Mantener la disponibilidad de conocimiento relevante, actual, validado y fiable para dar soporte a todas las actividades de los procesos y facilitar la toma de decisiones. Planificar la identificación, recopilación, organización, mantenimiento, uso y retirada de conocimiento.	
Declaración de Propósito del Proceso COBIT 5 Proporcionar el conocimiento necesario para dar soporte a todo el personal en sus actividades laborales, para la toma de decisiones bien fundadas y para aumentar la productividad.	

BAI08 Objetivos y Métricas de Proceso específicos de Seguridad	
Objetivos de Proceso específicos de Seguridad	**Métricas Relacionadas**
1. Se asegura la compartición del conocimiento con las salvaguardas adecuadas.	• Número de eventos de fuga de información • Número de empleados formados en seguridad de la información • Porcentaje de categorías de seguridad de la información cubiertas

BAI08 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
Práctica de Gestión	**Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)**		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
	De	**Descripción**	**Descripción**	**A**
BAI08.01 Cultivar y facilitar una cultura de intercambio de conocimientos. Concebir e implantar un esquema para cultivar y facilitar una cultura de intercambio de conocimientos.	APO01.04	Programa de concienciación y formación en seguridad de la información	Medidas de prevención de pérdida de información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que existen medidas adecuadas de prevención de pérdida de la información.				
2. Proporcionar formación para la concienciación en seguridad de la información en relación al intercambio de información.				
3. Incorporar consideraciones de seguridad de la información en el ciclo de vida de la información corporativa.				
Práctica de Gestión	**Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)**		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
	De	**Descripción**	**Descripción**	**A**
BAI08.02 Identificar y clasificar las fuentes de información. Identificar, validar y clasificar las diversas fuentes de información interna y externa necesarias para posibilitar el uso y la operación efectivos de los procesos de negocio y los servicios de TI.			Clasificación de fuentes de información actualizada	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Dar soporte al uso y al intercambio de información en relación a su clasificación y sensibilidad.				
2. Desarrollar una estructura para categorizar los sistemas.				
3. Desarrollar una estructura para clasificar la información.				
Práctica de Gestión	**Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)**		**Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)**	
	De	**Descripción**	**Descripción**	**A**
BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento. Organizar la información basándose en criterios de clasificación. Identificar y crear relaciones significativas entre elementos de información y facilitar el uso de la información. Identificar propietarios y definir e implementar niveles de acceso a los recursos de información.			Repositorios de conocimiento publicados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Mapear roles con áreas de conocimiento y asegurar que se han establecido controles de acceso apropiados para la información relevante.				

BAI08 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI08.04 Utilizar y compartir el conocimiento. Difundir las fuentes de conocimiento disponibles entre las partes interesadas relevantes y comunicar cómo estos recursos pueden ser utilizados para tratar diferentes necesidades (ej. resolución de problemas, aprendizaje, planificación estratégica y toma de decisiones).			Control de acceso actualizado	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que existen medidas adecuadas para la prevención de la pérdida de información.				
2. Implementar controles de acceso mediante el uso de políticas y procesos que restrinjan el uso y el intercambio no autorizado de información.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI08.05 Evaluar y retirar la información. Medir el uso y evaluar la actualización y relevancia de la información. Retirar la información obsoleta.			Reglas actualizadas para la eliminación de la información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Deshacerse de forma segura de la información. Incluir el borrado de datos de trazabilidad (datos personales/cuestiones de privacidad)				
2. Mantener y documentar una pista de auditoría solida/aceptada para la información.				
3. Alinear las medidas de seguridad de la información relevantes a la clasificación.				
4. Desarrollar políticas y procesos de destrucción segura de la información.				

Para más información respecto de los catalizadores relacionados, por favor consultar:
- Apéndice E. Guía Detallada: Catalizador de Información

BAI09 Gestionar los Activos	Área: Gestión Dominio: Construir, Adquirir e Implantar
Descripción del Proceso COBIT 5 Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia.	
Declaración de Propósito del Proceso COBIT 5 Contabilización de todos los activos de TI y optimización del valor proporcionado por estos activos.	

BAI09 Objetivos y Métricas de Proceso específicos de Seguridad	
Objetivos de Proceso específicos de Seguridad	**Métricas Relacionadas**
1. Todos los activos adquiridos cumplen con los requisitos de seguridad de la información.	• Frecuencia de revisión de los requerimientos de seguridad de la información
2. Se asignan roles y responsabilidades a todos los activos.	• Porcentaje de activos con propietarios asignados
3. Los mecanismos de seguridad de la información están en funcionamiento para evitar el uso no autorizado de los activos.	• Número de activos no autorizados identificados

BAI09 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
BAI09.01 Identificar y registrar los activos actuales.. Mantener un registro actualizado y exacto de todos los activos de TI necesarios para la prestación de servicios y garantizar su alineación con la gestión de la configuración y la administración financiera.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Inventario de activos	Requerimientos de seguridad de la información para los activos TI	BAI09.02
			Resultados de la comprobación física del inventario	DSS05.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Identificar dependencias entre los activos.				
2. Identificar los requisitos de seguridad de la información para los activos actuales y considerar las dependencias.				
3. Abordar la seguridad de la información para los activos TI, datos y formularios, etc.				

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
BAI09.02 Gestionar Activos Críticos. Identificar los activos que son críticos en la provisión de capacidad de servicio y dar los pasos para maximizar su fiabilidad y disponibilidad para apoyar las necesidades del negocio.	BAI09.01	Requerimientos de seguridad de la información para los activos TI	Niveles de criticidad de los activos de TI	BAI09.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir los niveles de criticidad e identificar la criticidad de los activos en un registro de activos.				
2. Hacer cumplir los requisitos de seguridad de la información de los activos.				

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
BAI09.03 Gestionar el ciclo de vida de los activos. Gestionar los activos desde su adquisición hasta su eliminación para asegurar que se utilizan tan eficaz y eficientemente como sea posible y son contabilizados y protegidos físicamente.	BAI09.02	Niveles de criticidad de los activos TI	Procedimientos de gestión de activos actualizados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Identificar y comunicar el riesgo de incumplimientos de seguridad de la información en relación al ciclo de vida de los activos.				
2. Asegurar que las medidas y los requerimientos de seguridad de la información se cumplen durante todo el ciclo de vida.				

BAI09 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI09.04 Optimizar el coste de los activos. Revisar periódicamente la base global de activos para identificar maneras de optimizar los costes y mantener el alineamiento con las necesidades del negocio.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
BAI09.05 Administrar Licencias. Administrar las licencias de software de forma que se mantenga el número óptimo de licencias para soportar los requerimientos de negocio y el número de licencias en propiedad sea suficiente para cubrir el software instalado y en uso.			Registro actualizado de licencias de software	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Establecer un procedimiento para el control de las instalaciones de software y otros activos de TI.				
2. Realizar verificaciones periódicas de la red para detectar software no autorizado.				

Para más información respecto de los relacionados, por favor consultar:
- Apéndice E. Guía Detallada: Catalizador de Información
- Apéndice F. Guía Detallada: Catalizador de Servicios, Infraestructura y Aplicaciones
- Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias; G.5 Operaciones de Seguridad de la Información

BAI10 Gestionar la Configuración	Área: Gestión Dominio: Construir, Adquirir e Implementar
Descripción del Proceso COBIT 5 Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarios para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.	
Declaración de Propósito del Proceso COBIT 5 Proporcionar suficiente información sobre los activos de servicio para que el servicio pueda gestionarse con eficacia, evaluar el impacto de los cambios y hacer frente a los incidentes de servicio.	

BAI10 Objetivos y Métricas de Proceso específicos de Seguridad	
Objetivos de Proceso específicos de Seguridad	**Métricas Relacionadas**
1. Se aprueban, implementan y mantienen en toda la empresa líneas de referencia de configuración de seguridad de la información.	• Número de veces que se han revisado y validado las líneas de referencia basado en un lapso predeterminado o cambios importantes y tiempo transcurrido • Número de discrepancias entre las líneas de referencia estándar de seguridad de la información y las configuraciones reales

BAI10 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI10.01 Establecer y mantener un modelo de configuración. Establecer y mantener un modelo lógico de la infraestructura, activos y servicios y la forma de registrar los elementos de configuración (CIs del inglés, *configuration items*) y las relaciones entre ellos. Incluyendo los CIs considerados necesarios para gestionar eficazmente los servicios y proporcionar una sola descripción fiable de los activos en un servicio.			Alertas de seguridad de la información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI10.02 Establecer y mantener un repositorio de configuración y una línea de referencia Establecer y mantener un repositorio de gestión de la configuración y crear unas bases de referencia de configuración controladas.			Informe de evaluación de vulnerabilidades	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Incluir una configuración de seguridad de la información para los elementos configurables como servidores/hardware, dispositivos de red y dispositivos finales.				
2. Identificar requerimientos de seguridad de la información para los activos actuales y tener en cuenta las dependencias.				
3. Supervisar el cumplimiento con las líneas de referencia de configuración de seguridad establecidas y aprobadas y con sus actualizaciones.				

Práctica de Gestión	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
	De	Descripción	Descripción	A
BAI10.03 Mantener y controlar los elementos de configuración. Mantener un repositorio actualizado de elemento de configuración rellenado con los cambios.			Plan de gestión de la configuración	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

BAI10 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	De	Descripción	Descripción	A
BAI10.04 Generar informes de estado y de configuración. Definir y elaborar informes de configuración sobre cambios en el estado de los elementos de configuración.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
	Entradas especificas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas especificas de seguridad (Adicionales a las Salidas COBIT 5)	
Práctica de Gestión	De	Descripción	Descripción	A
BAI10.05 Verificar y revisar la integridad del repositorio de configuración. Revisar periódicamente el repositorio de configuración y verificar la integridad y exactitud con respecto al objetivo deseado.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

Para más información respecto de los relacionados, por favor consultar:
- Apéndice F. Guía Detallada: Catalizador de Servicios, Infraestructura y Aplicaciones
- Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias; G.5 Operaciones de Seguridad de la Información

B.4 Entrega, Servicio y Soporte (DSS)

01 Gestionar operaciones.

02 Gestionar peticiones e incidentes de servicio.

03 Gestionar problemas.

04 Gestionar la continuidad.

05 Gestionar servicios de seguridad.

06 Gestionar controles de procesos de negocio.

Página dejada en blanco intencionadamente

DSS01 Gestionar Operaciones	Área: Gestión Dominio: Entrega, Servicio y Soporte
Descripción del Proceso de COBIT 5 Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.	
Declaración del Propósito del Proceso de COBIT 5 Entregar los resultados del servicio operativo de TI, según lo planificado.	

DSS01 Objetivos y Métricas del Proceso específicas de Seguridad	
Objetivos de Proceso específicos de Seguridad	**Métricas Relacionadas**
1. Las operaciones de seguridad de la información son realizadas de acuerdo a un plan operativo de seguridad de la información, en línea con la estrategia de seguridad de la información	• Número de incidentes de seguridad de la información causados por problemas operativos
2. Los estándares de seguridad de la información aplicables están identificados y se cumplen	• Número de cuestiones de seguridad de la información no contempladas por estándares de seguridad de la información • Número de estándares de seguridad de la información no abordados o satisfechos por el plan operativo de seguridad de la información

DSS01 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso

Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
DSS01.01 Ejecutar procedimientos operativos. Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.	APO03.05	Guía de implementación del servicio de arquitectura de seguridad de la información	Procedimientos operativos de seguridad de la información	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Verificar que los procedimientos operativos de seguridad de la información relevantes están incluidos en los procedimientos operativos ordinarios.				
2. Asegurar que el ciclo de vida de procesamiento de la información (recepción, procesamiento, almacenamiento y salida) incorpora la política de seguridad de la información y los requerimientos regulatorios.				
3. Asegurar que las operaciones de seguridad de la información son planificadas, ejecutadas y controladas de acuerdo con el plan operativo.				
4. Aplicar seguridad de la información y derechos de acceso a todos los datos.				

Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
DSS01.02 Gestionar servicios externalizados de TI. Gestionar la operación de servicios externalizados de TI para mantener la protección de la información empresarial y la confiabilidad de la entrega del servicio.	APO01.03	Políticas de seguridad de la información y afines	Planes de aseguramiento de terceros	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar y supervisar activamente el cumplimiento de terceros con las políticas, estándares y requerimientos de seguridad de la información de la empresa.				

Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
DSS01.03 Supervisar la infraestructura de TI. Supervisar la infraestructura TI y los eventos relacionados con ella. Almacenar la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo de las operaciones y las actividades relacionadas con el soporte a esas operaciones.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Reglas de monitorización de activos y estado de eventos	Reglas de monitorización de activos actualizadas	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que TI supervisa activamente aspectos de seguridad de la información de la infraestructura de TI, tales como configuración, operaciones, acceso y uso.				

DSS01 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso (cont.)				
Prácticas de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
	De	**Descripción**	**Descripción**	**A**
DSS01.04 Gestionar el entorno. Mantener las medidas para la protección contra factores ambientales. Instalar equipamiento y dispositivos especializados para supervisar y controlar el entorno.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Políticas de seguridad ambiental	Políticas de seguridad ambiental actualizadas	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que la gestión del entorno se adhiere a los requerimientos de seguridad de la información.				
Prácticas de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
	De	**Descripción**	**Descripción**	**A**
DSS01.05 Gestionar las instalaciones. Gestionar las instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Informes de evaluación de instalaciones	Informes de evaluación de instalaciones actualizados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que la gestión de instalaciones se adhiere a los requerimientos de seguridad de la información.				

Para más información sobre catalizadores relacionados, consultar:
- Apéndice F. Guía Detallada: Catalizador de Servicios, Infraestructuras y Aplicaciones.
- Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias, G.5. Operaciones e Seguridad de la Información.

DSS02 Gestionar Peticiones e Incidentes de Servicio	Área: Gestión Dominio: Entrega, Servicio y Soporte
Descripción del Proceso de COBIT 5 Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.	
Declaración del Propósito del Proceso de COBIT 5 Lograr una mayor productividad y minimizar las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.	

DSS02 Objetivos y Métricas del Proceso específicas de Seguridad	
Objetivos del Proceso específicos de Seguridad	**Métricas Relacionadas**
1. Se ha establecido y se mantiene un programa de respuesta ante incidentes de seguridad de la información	• Tiempo promedio de resolución de incidencias de seguridad • Número y porcentaje de incidentes relacionados con seguridad de la información que causan interrupción en los procesos críticos de negocio • Número de incidentes de seguridad de la información abiertos/cerrados y sus niveles de riesgo • Frecuencia de pruebas del plan de respuesta ante incidentes de seguridad de la información

DSS02 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso

Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio. Definir esquemas y modelos de clasificación de incidentes y peticiones de servicio.	APO01.03	Políticas de seguridad de la información y afines	Esquema de clasificación de incidentes de seguridad de la información	DSS02.02
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir y comunicar la naturaleza y las características de los potenciales incidentes relacionados con seguridad para que puedan ser fácilmente reconocidos y su impacto entendido y, así, permitir una respuesta adecuada.				
Prácticas de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
	De	**Descripción**	**Descripción**	**A**
DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes. Identificar, registrar y clasificar peticiones de servicio e incidentes, y asignar una prioridad según la criticidad del negocio y los acuerdos de servicio.	DSS02.01	Esquema de clasificación de incidentes de seguridad de la información	Incidentes y peticiones de servicio de seguridad de la información clasificados y priorizados	APO08.03 APO12.01 APO13.03 DSS02.07
	DSS05.07	Tiques de incidentes de seguridad		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Mantener un procedimiento de investigación y respuesta de incidentes de seguridad de la información. Asegurar que se han puesto medidas para proteger la confidencialidad de la información relativa a incidentes de seguridad y que todo el personal está al corriente del procedimiento.				
Prácticas de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
	De	**Descripción**	**Descripción**	**A**
DSS02.03 Verificar, aprobar y resolver peticiones de servicio. Seleccionar los procedimientos adecuados para peticiones y verificar que las peticiones de servicio cumplen los criterios de petición definidos.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

DSS02 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
Prácticas de Gestión	**De**	**Descripción**	**Descripción**	**A**
DSS02.04 Investigar, diagnosticar y localizar incidentes. Identificar y registrar síntomas de incidentes, determinar posibles causas y asignar recursos a su resolución.			Procedimientos de recogida de evidencias	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Mantener un procedimiento de recogida de evidencias en línea con las normas de evidencias forenses locales y asegurar que todo el personal está al corriente del procedimiento.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
Prácticas de Gestión	**De**	**Descripción**	**Descripción**	**A**
DSS02.05 Resolver y recuperarse ante incidentes. Documentar, solicitar y probar las soluciones identificadas o temporales y ejecutar acciones de recuperación para restaurar el servicio TI relacionado.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Análisis de impacto en el negocio, política de gestión del riesgo organizativo, esquema de clasificación de incidentes	Plan de respuesta ante incidentes	DSS02.07
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Definir un plan de respuesta ante incidentes de seguridad de la información.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
Prácticas de Gestión	**De**	**Descripción**	**Descripción**	**A**
DSS02.06 Cerrar peticiones de servicio e incidentes. Verificar la satisfactoria resolución de incidentes y/o satisfactorio cumplimiento de peticiones, y cierre.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
Prácticas de Gestión	**De**	**Descripción**	**Descripción**	**A**
DSS02.07 Seguir el estado y emitir de informes. Hacer seguimiento, analizar e informar de incidentes y tendencias de cumplimiento de peticiones, regularmente, para proporcionar información para la mejora continua.	DSS02.02	Incidentes y peticiones de servicio de seguridad de la información clasificados y priorizados	Lecciones aprendidas	Interno
	DSS02.05	Plan de respuesta ante incidentes		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Reportar los resultados de las investigaciones de incidentes de seguridad a los grupos de interés oportunos, incluyendo informes periódicos a la dirección ejecutiva.				
2. Asegurar que los incidentes de seguridad y las acciones de seguimiento oportunas, incluyendo análisis de la causa raíz, siguen los procesos de gestión de problemas e incidentes existentes.				

Para más información sobre catalizadores relacionados, consultar:
- Apéndice E. Guía Detallada: Catalizador de Información, E.9. Cuadro de Mando de Seguridad de la Información
- Apéndice F. Guía Detallada: Catalizador de Servicios, Infraestructuras y Aplicaciones.
- Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias, G.5. Operaciones e Seguridad de la Información.

DSS03 Gestionar Problemas	Área: Gestión Dominio: Entrega, Servicio y Soporte
Descripción del Proceso de COBIT 5 Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.	
Declaración del Propósito del Proceso de COBIT 5 Incrementar la disponibilidad, mejorar los niveles de servicio, reducir costes, y mejorar la comodidad y satisfacción del cliente reduciendo el número de problemas operativos..	

DSS03 Objetivos y Métricas del Proceso específicas de Seguridad	
Objetivos del Proceso específicos de Seguridad	**Métricas Relacionadas**
1. Los problemas de seguridad de la información son resueltos de una forma sostenible	• Número de problemas de seguridad de la información recurrentes que permanecen sin resolver. • Número de problemas relativos a seguridad de la información para los que se ha encontrado una solución satisfactoria que contempla cuestiones críticas de seguridad de la información

DSS03 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso

Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
DSS03.01 Identificar y clasificar problemas. Definir e implementar criterios y procedimientos para informar de los problemas identificados, incluyendo clasificación, categorización y priorización de problemas.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Análisis de vulnerabilidades	Esquema de clasificación de problemas de seguridad de la información	DSS03.04
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Clasificar, categorizar y priorizar los problemas de seguridad de la información.				

Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
DSS03.02 Investigar y diagnosticar problemas. Investigar y diagnosticar problemas utilizando expertos en las materias relevantes para valorar y analizar las causas raíz.			Causas raíz de los problemas actualizadas	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Investigar los problemas de seguridad de la información.				

Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
DSS03.03 Levantar errores conocidos. Tan pronto como las causas raíz de los problemas se hayan identificado, crear registros de errores conocidos y una solución temporal apropiada, e identificar soluciones potenciales.			Registros de errores conocidos actualizados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Escalar los problemas de seguridad de la información cuando sea necesario.				

Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
DSS03.04 Resolver y cerrar problemas. Identificar e iniciar soluciones sostenibles refiriéndose a la causa raíz, levantando peticiones de cambio a través del proceso de gestión de cambios establecido si se requiere para resolver errores. Asegurarse de que el personal afectado está al tanto de las acciones tomadas y de los planes desarrollados para prevenir que vuelvan a ocurrir futuros incidentes.	DSS03.01	Esquema de clasificación de problemas de seguridad de la información	Causa raíz de los problemas	DSS03.05
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Realizar análisis de causa raíz, resolver problemas de seguridad de la información y actualizar el plan de respuesta ante incidentes. Hacer seguimiento y registrar los problemas de seguridad de la información.				

DSS03 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
Prácticas de Gestión	**De**	**Descripción**	**Descripción**	**A**
DSS03.05 Realizar una gestión de problemas proactiva. Recoger y analizar datos operacionales (especialmente registros de incidentes y cambios) para identificar tendencias emergentes que puedan indicar problemas. Registrar problemas para permitir la valoración.	DSS03.04	Causa raíz de problemas	Implementación de políticas y procedimientos de seguridad de la información y planes de acción para abordar las causas raíz.	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Analizar y aprovechar las lecciones aprendidas.				

Para más información sobre catalizadores relacionados, consultar:
- Apéndice E. Guía Detallada: Catalizador de Información, E.9. Cuadro de Mando de Seguridad de la Información
- Apéndice F. Guía Detallada: Catalizador de Servicios, Infraestructuras y Aplicaciones.
- Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias, G.5. Operaciones e Seguridad de la Información.

DSS04 Gestionar la Continuidad	Área: Gestión Dominio: Entrega, Servicio y Soporte
Descripción del Proceso de COBIT 5 Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.	
Declaración del Propósito del Proceso de COBIT 5 Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa.	

DSS04 Objetivos y Métricas del Proceso específicas de Seguridad	
Objetivos del Proceso específicos de Seguridad	**Métricas Relacionadas**
1. El riesgo de la información se ha identificado adecuadamente y se incluye en los planes de continuidad de las tecnologías de la información y comunicaciones (TIC)	• Número de invocaciones al plan causadas por incidentes de seguridad de la información • Número de incidentes de seguridad de la información escalados para la activación de la continuidad TIC • Número de sistemas de seguridad de la información críticos cubiertos por el plan de continuidad TIC.

DSS04 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso

Prácticas de Gestión	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
DSS04.01 Definir la política de continuidad de negocio, objetivos y alcance. Definir la política y alcance de continuidad de negocio alineada con los objetivos de negocio y de las partes interesadas.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Política para la continuidad de negocio	Política para la continuidad de negocio actualizada	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que la seguridad de la información forma parte del ciclo de vida de la continuidad de negocio.				
DSS04.02 Mantener una estrategia de continuidad. Evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Análisis de impacto en el negocio (AIN)	Análisis de impacto en el negocio (AIN) actualizado	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Incluir escenarios que tengan en cuenta la seguridad de la información.				
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio. Desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con sus actividades críticas	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Plan de continuidad de negocio (PCN)	Plan de continuidad de negocio (PCN) actualizado	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Incluir requerimientos de seguridad de la información en el plan de continuidad de negocio (PCN).				
DSS04.04 Ejercitar, probar y revisar el BCP. Probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

DSS04 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
Prácticas de Gestión	**De**	**Descripción**	**Descripción**	**A**
DSS04.05 Revisar, mantener y mejorar el plan de continuidad. Realizar una revisión por la Dirección de la capacidad de continuidad a intervalos regulares para asegurar su continua idoneidad, adecuación y efectividad. Gestionar los cambios en el plan de acuerdo al proceso de control de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja continuamente los requerimientos actuales del negocio.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Plan de continuidad de negocio (PCN)	Plan de continuidad de negocio (PCN) actualizado	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Considerar los incidentes de seguridad de la información como disparadores importantes para mejorar el plan de continuidad de negocio (PCN)				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
Prácticas de Gestión	**De**	**Descripción**	**Descripción**	**A**
DSS04.06 Proporcionar formación en el plan de continuidad. Proporcionar a todas las partes implicadas, internas y externas, de sesiones formativas regulares que contemplen los procedimientos y sus roles y responsabilidades en caso de disrupción.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
Prácticas de Gestión	**De**	**Descripción**	**Descripción**	**A**
DSS04.07 Gestionar acuerdos de respaldo. Mantener la disponibilidad de la información crítica del negocio.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Resultados de pruebas de datos de respaldo	Resultados de pruebas de datos de respaldo actualizados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asegurar que los acuerdos de copia de respaldo y recuperación incluyen requerimientos de seguridad de la información.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
Prácticas de Gestión	**De**	**Descripción**	**Descripción**	**A**
DSS04.08 Ejecutar revisiones post-reanudación. Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Informes de revisión post-reanudación	Informes de revisión post-reanudación actualizados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
10. Asegurar que las revisiones pos-reanudación incluyen la seguridad de la información.				

Para más información sobre catalizadores relacionados, consultar:
- Apéndice A: Guía Detallada: Catalizador de Principios, Políticas y Marcos.

DSS05 Gestionar Servicios de Seguridad	Área: Gestión Dominio: Entrega, Servicio y Soporte
Descripción del Proceso de COBIT 5 Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.	
Declaración del Propósito del Proceso de COBIT 5 Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.	

DSS05 Objetivos y Métricas del Proceso específicas de Seguridad	
Objetivos del Proceso específicos de Seguridad	**Métricas Relacionadas**
1. La seguridad de las redes y las comunicaciones cubre con las necesidades del negocio.	• Número de vulnerabilidades descubiertas • Número de rupturas (*breaches*) de cortafuegos
2. La información procesada, almacenada y transmitida en los dispositivos de usuario finales está protegida.	• Porcentaje de individuos que reciben formación de concienciación relativa al uso de dispositivos de usuario finales • Número de incidentes que impliquen dispositivos de usuario finales • Número de dispositivos de usuario finales no autorizados detectados en la red o en el entorno
3. Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio.	• Promedio de tiempo entre los cambios y actualizaciones de cuentas • Número de cuentas (con respecto al número de usuarios/empleados autorizados)
4. Se han implantado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida.	• Porcentaje de pruebas periódicas de los dispositivos de seguridad del entorno • Clasificación media para las evaluaciones de seguridad física • Número de incidentes relacionados con seguridad física
5. La información electrónica tiene las medidas de seguridad apropiadas mientras está almacenada, transmitida o destruida.	• Número de incidentes relacionados con accesos no autorizados a la información

DSS05 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
Prácticas de Gestión	**De**	**Descripción**	**Descripción**	**A**
DSS05.01 Proteger contra software malicioso (*malware*). Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware- y correo basura).			Política de prevención de software malicioso	APO01.04
			Evaluaciones de amenazas potenciales	APO12.02 APO12.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención.				
2. Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automática o semi-automáticamente).				
3. Distribuir todo el software de protección de forma centralizada (versión y nivel de parcheado) usando una configuración centralizada y la gestión de cambios.				
4. Revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).				
5. Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada (por ejemplo, software espía y correos de *phishing*).				
6. Realizar formación periódica sobre software malicioso en el uso del correo electrónico e Internet. Formar a los usuarios para no instalarse software compartido o no autorizado.				

DSS05 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
Prácticas de Gestión	**De**	**Descripción**	**Descripción**	**A**
DSS05.02 Gestionar la seguridad de la red y las conexiones. Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.	APO01.06	Guías de clasificación de la información	Política de seguridad en la conectividad	APO01.04
	APO09.03	ANSs	Resultados de las pruebas de intrusión	MEA02.08
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones.				
2. Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña.				
3. Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente.				
4. Cifrar la información en tránsito de acuerdo con su clasificación.				
5. Aplicar los protocolos de seguridad aprobados a las conexiones de red.				
6. Configurar los equipamientos de red de forma segura.				
7. Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.				
8. Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.				
9. Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
Prácticas de Gestión	**De**	**Descripción**	**Descripción**	**A**
DSS05.03 Gestionar la seguridad de los puestos de usuario finales. Asegurar que los puestos de usuario finales (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.	APO03.02	Modelo de arquitectura de la información	Políticas de seguridad para dispositivos de usuario finales	APO01.04
	APO09.03	• Acuerdos de Nivel de Servicio (ANSs) • Acuerdos de Nivel Operativo (OLAs)		
	BAI09.01	Resultados de pruebas de inventarios físicos		
	DSS06.06	Informes de violaciones		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Configurar los sistemas operativos de forma segura.				
2. Implementar mecanismos de bloqueo de los dispositivos.				
3. Cifrar la información almacenada de acuerdo a su clasificación.				
4. Gestionar el acceso y control remoto.				
5. Gestionar la configuración de la red de forma segura.				
6. Implementar el filtrado del tráfico de la red en dispositivos de usuario finales.				
7. Proteger la integridad del sistema.				
8. Proveer de protección física a los dispositivos de usuario finales.				
9. Deshacerse de los dispositivos de usuario finales de forma segura.				

DSS05 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
Prácticas de Gestión	**De**	**Descripción**	**Descripción**	**A**
DSS05.04 Gestionar la identidad del usuario y el acceso lógico. Asegurar que todos los usuarios tienen derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio.	APO01.02	Definición de roles y responsabilidades relacionados con TI	• Resultados de las revisiones de cuentas de usuarios y privilegios de los usuarios • Derechos de acceso de usuarios aprobados	Interno
	APO03.02	Modelo de arquitectura de la información		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menos privilegio, necesidad de tener y necesidad de conocer.				
2. Identificar unívocamente todas las actividades de proceso de la información por los roles funcionales, coordinación con las unidades de negocio y asegurando que todos los roles están definidos consistentemente, incluyendo roles definidos por el propio negocio en las aplicaciones de procesos de negocio.				
3. Autenticar todos los accesos a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de negocio que gestionan la autenticación en las aplicaciones usadas en los procesos de negocio para asegurar que los controles de autenticación han sido administrados adecuadamente.				
4. Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.				
5. Segregar y gestionar cuentas de usuarios privilegiadas.				
6. Realizar regularmente revisiones de la gestión de todas las cuentas y privilegios relacionados.				
7. Asegurar que todos los usuarios (internos , externos y temporales) y su actividad en los sistemas TI (aplicaciones de negocio, infraestructura TI, operación , desarrollo y mantenimiento de sistemas) son identificables unívocamente. Identificar unívocamente todas las actividades de procesamiento de la información por usuario.				
8. Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
Prácticas de Gestión	**De**	**Descripción**	**Descripción**	**A**
DSS05.05 Gestionar el acceso físico a los activos de TI. Definir e implementar procedimientos para conceder, limitar y revocar el acceso a los locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, personal temporal, clientes, proveedores, visitantes o cualquier otra tercera parte.			Registros de acceso	DSS06.03
			Peticiones de acceso aprobadas	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. Las peticiones formales de acceso deberán ser completadas y autorizadas por la dirección del emplazamiento de TI, y conservarse las solicitudes registradas .Los formularios deberían identificar específicamente las áreas a las que el individuo tiene acceso concedido.				
2. Asegurar que los perfiles de acceso están actualizados. El acceso a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) debe basarse en función del trabajo y responsabilidades.				
3. Rregistrar y supervisar todos los puntos de entrada a los emplazamientos de TI. Registrar todos los visitantes a las dependencias, incluyendo contratistas y proveedores.				
4. Instruir a todo el personal para mantener visible la identificación en todo momento. Prevenir la expedición de tarjetas o placas de identidad sin la autorización adecuada.				
5. Escoltar a los visitantes en todo momento mientras estén en las dependencias . Si se encuentra a un individuo que no va acompañado, que no resulta familiar y que no lleva visible la identificación de empleado, se deberá alertar al personal de seguridad.				
6. Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros y dispositivos de seguridad en puertas interiores y exteriores. Asegurar que los dispositivos restringen el acceso y disparen una alarma en caso de acceso no autorizado. Ejemplos de estos dispositivos incluyen placas o tarjetas de acceso, teclados (keypads), circuitos cerrados de televisión y escáneres biométricos.				
7. Realizar regularmente formación de concienciación de seguridad física.				

DSS05 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
Prácticas de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
	De	**Descripción**	**Descripción**	**A**
DSS05.06 Gestionar documentos sensibles y dispositivos de salida. Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (tokens) de seguridad.	APO03.02	Modelo de arquitectura de la información	• Privilegios de acceso • Inventario de documentos y dispositivos sensibles.	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida hacia, dentro y fuera de la empresa.				
2. Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basándose en el principio del menor privilegio, equilibrando riesgo y requerimientos del negocio.				
3. Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones.				
4. Establecer salvaguardas física apropiadas sobre formularios especiales y dispositivos sensibles.				
5. Destruir la información sensible y proteger los dispositivos de salida (por ejemplo, desmagnetizando los soportes magnéticos, destruyendo físicamente los dispositivos de memoria, poniendo trituradoras o papeleras cerradas para destruir formularios especiales y otros documentos confidenciales).				
Prácticas de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
	De	**Descripción**	**Descripción**	**A**
DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad. Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.			Tiques de incidentes de seguridad	DSS02.02
			• Características de incidentes de seguridad • Registros de incidentes de seguridad	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Registrar los eventos relacionados con la seguridad reportados por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo . Retenerla durante un período apropiado para ayudar en futuras investigaciones.				
2. Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta acorde.				
3. Revisar regularmente los registros de eventos para detectar incidentes potenciales.				
4. Mantener un procedimiento para la recopilación de evidencias en línea con las normas de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos.				
5. Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.				

DSS06 Gestionar Controles de Proceso de Negocio	Área: Gestión Dominio: Entrega, Servicio y Soporte
Descripción de Proceso COBIT 5 Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.	
Declaración del Propósito del Proceso COBIT 5 Mantener la integridad de la información y la seguridad de los activos de información manejados en los procesos de negocio dentro de la empresa o externalizados.	

DSS06 Objetivos y métricas de procesos específicos de seguridad	
Objetivos de Proceso específicos de seguridad	**Métricas Relacionadas**
1. Se han establecido, revisado y actualizado controles apropiados sobre los procesos de seguridad de la información.	• Porcentaje de las medidas de la seguridad de la información que se han implementado adecuadamente o siguen siendo válidas.
2. Se han establecido controles adecuados para proteger la confidencialidad, integridad y disponibilidad de los procesos de negocio.	• Número de incidentes relacionados con la seguridad de la información causados porque los controles de seguridad de la información establecidos no eran los adecuados.

DSS06 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
Prácticas de Gestión	**De**	**Descripción**	**Descripción**	**A**
DSS06.01 Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos. Evaluar y supervisar continuamente la ejecución de las actividades de los procesos de negocio y controles relacionados, basados en el riesgo corporativo, para asegurar que el procesamiento de controles está alineado con las necesidades del negocio.			Controles de aplicación segura	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Identificar y priorizar los procesos de seguridad de la información de acuerdo con el riesgo de negocio, cumplimiento, etc.				
2. Identificar los requisitos específicos de seguridad de la información operacionales (por ejemplo, cumplimiento).				
3. Identificar e implementar los controles de aplicación necesarios.				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
Prácticas de Gestión	**De**	**Descripción**	**Descripción**	**A**
DSS06.02 Controlar el procesamiento de la información. Operar la ejecución de las actividades de proceso de negocio y controles relacionados, basados en el riesgo corporativo, para asegurar que el procesamiento de la información es válido, completo, preciso, oportuno y seguro (es decir, refleja el uso de negocio autorizado y legitimado).				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

DSS06 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
Prácticas de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
	De	**Descripción**	**Descripción**	**A**
DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización. Gestionar los roles de negocio, responsabilidades, niveles de autoridad y segregación de tareas necesarias para apoyar los objetivos del proceso de negocio. Autorizar el acceso a cualquier activo de información relativo a los procesos de información del negocio, incluyendo aquellos bajo la custodia del negocio, de TI y de terceras partes. Esto asegura que el negocio sabe dónde están los datos y quién los está manejando en su nombre.	APO13.01	Declaración de alcance del SGSI	Roles, responsabilidades , privilegios de acceso y niveles de autorización actualizados	Interno
	DSS05.05	Registro de accesos		
	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Funciones y responsabilidades asignadas		
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Gestionar los roles, responsabilidades, privilegios de acceso y niveles de autoridad para la información.				
2. Asignar derechos de acceso basados en los principios de la necesidad de conocer ,mínimo privilegio y en los requisitos de los puestos.				
3. Borrar/eliminar los derechos de acceso cuando los usuarios dejan lasposiciones/unidades.				
4. Implementar la separación de funciones de acuerdo con los procesos de negocio para evitar el fraude y accesos no autorizados.				
5. Hacer seguimiento de las autorizaciones.				
Prácticas de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
	De	**Descripción**	**Descripción**	**A**
DSS06.04 Gestionar errores y excepciones. Gestionar las excepciones y errores de los procesos de negocio y facilitar su corrección. Incluir escalada errores y excepciones en los procesos de negocio y la ejecución de acciones correctivas definidas. Esto proporciona garantía de precisión e integridad del proceso de información del negocio.			Privilegios de acceso actualizados	Interno
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Asignar/retirar permisos de acceso en situaciones de emergencia.				
Prácticas de Gestión	**Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
	De	**Descripción**	**Descripción**	**A**
DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades y de información. Asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan. Esto permite trazabilidad de la información a lo largo de su ciclo de vida y procesos relacionados. Proporciona garantías de que la información que conduce el negocio es de confianza y ha sido procesada acorde a los objetivos definidos.				
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.				

DSS06 Prácticas, Entradas/Salidas y Actividades específicos de Seguridad del Proceso *(cont.)*				
	Entradas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		**Salidas específicas de Seguridad (Adicionales a las Entradas de COBIT 5)**	
Prácticas de Gestión	**De**	**Descripción**	**Descripción**	**A**
DSS06.06 Asegurar los activos de información. Asegurar los activos de información accesibles por el negocio a través de los métodos aprobados, incluyendo la información en formato electrónico (tales como métodos para crear nuevos activos en cualquier forma, dispositivos portátiles, aplicaciones de usuario y dispositivos de almacenamiento), información en formato físico (tales como documentos fuente o informes de salida) e información en tránsito. Esto beneficia al negocio proporcionando una salvaguarda de la información de comienzo a fin.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Inventario de activos	Informe de violaciones	DSS05.03
Actividades específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1, Hacer cumplir la clasificación de datos, el uso aceptable y las políticas y procedimientos de seguridad para soportar la protección de los activos de información.				

Para obtener más información acerca de los facilitadores relacionados, por favor consulte
- Apéndice C. Guía Detallada: Catalizador de Estructuras Organizativas, C.5. Custodios de Información / propietarios de negocio.
- Apéndice E. Guía Detallada: Catalizador de Información.

Página dejada en blanco intencionadamente

B.5 Supervisar, Evaluar y Valorar (MEA)

01 Supervisar, evaluar y valorar el rendimiento y la conformidad.

02 Supervisar, evaluar y valorar el sistema de control interno.

03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos.

Página dejada en blanco intencionadamente

MEA01 Supervisar, evaluar y valorar el rendimiento y la conformidad	Área: Gestión Dominio: Supervisar, Evaluar y Valorar
Descripción de Proceso COBIT 5 Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.	
Declaración del Propósito del Proceso COBIT 5 Proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.	

MEA01 Objetivos y métricas de procesos específicos de seguridad	
Objetivos de Proceso específicos de seguridad	**Métricas Relacionadas**
1. El rendimiento de la seguridad de la información es supervisado de forma continua.	• Porcentaje de los procesos de negocio que satisfacen los requerimientos de seguridad de la información definidos.
2. La seguridad de la información y las prácticas de riesgo de la información se ajustan a los requisitos de cumplimiento interno.	• Porcentaje de las prácticas de seguridad de la información que satisfacen los requerimientos de cumplimiento internos.

MEA01 Prácticas, Entradas/Salidas y Actividades de Procesos Específicos de Seguridad				
	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas específicas de seguridad (Adicionales a las Entradas COBIT 5)**	
Prácticas de Gobierno	**De**	**Descripción**	**Descripción**	**A**
MEA01.01 Establecer un enfoque de la supervisión. Involucrar a las partes interesadas en el establecimiento y mantenimiento de un enfoque de supervisión que defina los objetivos, alcance y método de medición de las soluciones de negocio, la entrega del servicio y la contribución a los objetivos de negocio. Integrar este enfoque con el sistema de gestión del rendimiento de la compañía.	APO01.03	Políticas de seguridad de la información y relacionadas.	Proceso y procedimiento de supervisión de la seguridad de la información	MEA01.02
	BAI02.01	Requerimientos de seguridad de la información.		
	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Estándares y regulaciones de seguridad de la información		
Actividades especificas de seguridad (Adicionales a las Entradas COBIT 5)				
1. Identificar y confirmar las partes interesados en seguridad de la información.				
2. Involucrar a las partes interesadas y comunicar los requisitos de la seguridad de la información y los objetivos de seguimiento y emisión de informes.				
3. Alinear y mantener continuamente el enfoque de supervisión y evaluación de la seguridad de información con los enfoques de TI y de la empresa.				
4. Establecer el proceso y el procedimiento de supervisión de la seguridad de información.				
5. Acordar un sistema de gestión del ciclo de vida y el proceso de control de cambios para la supervisión y emisión de informes de seguridad de información.				
6. Solicitar, priorizar y asignar recursos para supervisar la seguridad de información.				
	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas específicas de seguridad (Adicionales a las Entradas COBIT 5)**	
Prácticas de Gobierno	**De**	**Descripción**	**Descripción**	**A**
MEA01.02 Establecer los objetivos de cumplimiento y rendimiento. Colaborar con las partes interesadas en la definición, revisión periódica, actualización y aprobación de los objetivos de rendimiento y cumplimiento enmarcados dentro del sistema de medida del rendimiento.	MEA01.01	Procesos y procedimiento de supervisión de seguridad de la información	Acuerdos sobre métricas y objetivos de seguridad de la información	APO07.04 MEA01.04
Actividades especificas de seguridad (Adicionales a las Entradas COBIT 5)				
1. Definir los objetivos de rendimiento de seguridad de la información de acuerdo con los estándares globales de rendimiento de TI.				
2. Comunicar el rendimiento de seguridad de información y los objetivos de conformidad a las principales partes interesadas con la debida diligencia.				
3. Evaluar si los objetivos y las métricas de seguridad de la información son adecuadas, es decir, específicas, medibles, realizables, pertinentes y de duración determinada.				

MEA01 Prácticas, Entradas/Salidas y Actividades de Procesos Específicos de Seguridad *(cont.)*				
Prácticas de Gobierno	**Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)**		**Salidas específicas de seguridad (Adicionales a las Entradas COBIT 5)**	
	De	**Descripción**	**Descripción**	**A**
MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento. Recopilar y procesar datos oportunos y precisos de acuerdo con los enfoques del negocio.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Regulaciones aplicables	Datos de seguimiento procesados	Interno
Actividades especificas de seguridad (Adicionales a las Entradas COBIT 5)				
1 Recopilar y analizar los datos de rendimiento y de conformidad relativos a la seguridad de la información y a la gestión de riesgos de la información (por ejemplo, métricas de seguridad de la información, informes de seguridad de la información).				
2. Valorar la eficiencia, idoneidad e integridad de los datos recogidos.				
Prácticas de Gobierno	**Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)**		**Salidas específicas de seguridad (Adicionales a las Entradas COBIT 5)**	
	De	**Descripción**	**Descripción**	**A**
MEA01.04 Analizar e informar sobre el rendimiento. Revisar e informar de forma periódica sobre el desempeño respecto de los objetivos, utilizando métodos que proporcionen una visión completa y sucinta del rendimiento de las TI y encaje con el sistema corporativo de supervisión.	MEA01.02	Acuerdo sobre métricas y objetivos de seguridad de la información	Informes de seguridad de la información y planes de acciones correctivas actualizados	APO01.07
Actividades especificas de seguridad (Adicionales a las Entradas COBIT 5)				
1. Diseñar, implementar y acordar una serie de informes de desempeño de seguridad de la información.				
2. Comparar los valores de rendimiento con los objetivos y puntos de referencia internos y, cuando sea posible, con puntos de referencia externos (industria y competidores clave).				
Prácticas de Gobierno	**Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)**		**Salidas específicas de seguridad (Adicionales a las Entradas COBIT 5)**	
	De	**Descripción**	**Descripción**	**A**
MEA01.05 Asegurar la implantación de medidas correctivas. Apoyar a las partes interesadas en la identificación, inicio y seguimiento de las acciones correctivas para solventar anomalías.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Guías de escalado	Proceso de seguimiento de acciones correctivas en materia de seguridad de la información	Interno
Actividades especificas de seguridad (Adicionales a las Entradas COBIT 5)				
1. Desarrollar un proceso de seguimiento para las acciones correctivas en materia de seguridad de la información.				

Para obtener más información acerca de los facilitadores relacionados, por favor consulte
- Apéndice F. Guía Detallada: Catalizador de Servicios, Infraestructura y Aplicaciones, F.10, proporcionar seguimiento y servicios de alerta para eventos relacionados con la seguridad.
- Apéndice G. Guía Detallada: Catalizador de Personas, Habilidades y Competencias, G.6, evaluación de la información, pruebas y cumplimiento.

MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno	Área: Gestión Dominio: Supervisar, Evaluar y Valorar
Descripción del Proceso COBIT 5 Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.	
Declaración del Propósito del Proceso COBIT 5 Ofrecer transparencia a las partes interesadas claves respecto de la adecuación del sistema de control interno para generar confianza en las operaciones, en el logro de los objetivos de la compañía y un entendimiento adecuado del riesgo residual.	

MEA02 Objetivos y Métricas de Seguridad Específicos del Proceso	
Objetivos de Seguridad Específicos del Proceso	**Métricas Relacionadas**
1. Los controles de seguridad de la información están desplegados y operan eficazmente.	• Porcentaje de los procesos que satisfacen los requerimientos de control de seguridad de la información • Porcentaje de controles en los que se cumplen los requisitos de control de seguridad de la información
2. Hay establecidos procesos de monitorización para los controles de seguridad y se informa de sus resultados.	• Porcentaje de controles de seguridad de la información adecuadamente monitorizados con resultados informados y revisados

MEA02 Prácticas de Seguridad Específicos del Proceso, Entradas/Salidas y Actividades

Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas Específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
MEA02.01 Supervisar el control interno. Realizar, de forma continua, la supervisión, los estudios comparativos y la mejora el entorno de control de TI y el marco de control para alcanzar los objetivos organizativos.	APO01.03	Políticas de seguridad de la información y afines Informe de auditoría del SGSI	Alcance para el aseguramiento de seguridad de la información y estrategia de evaluación de controles internos definidos	MEA02.03
	APO13.03	Informe de auditoría ISMS		
	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Auditorías externas independientes		

Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)
1. Realizar una revisión periódica de las políticas y procedimientos de seguridad de la información.
2. Determinar el alcance del aseguramiento p.ej. controles de seguridad de la información a evaluar.
3. Establecer un enfoque formal para el aseguramiento de seguridad de la información.

Práctica de Gestión	Entradas Específicas de Seguridad (Adicionales a las Entradas de COBIT 5)		Salidas Específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio. Revisar la operación de controles, incluyendo la revisión de las evidencias de supervisión y pruebas, para asegurar que los controles incorporados en los procesos de negocio operan de manera efectiva. Incluir actividades de mantenimiento de evidencias de la operación efectiva de controles a través de mecanismos como la comprobación periódica de controles, supervisión continua de controles, evaluaciones independientes, centros de mando y control y centros de operación de red. Esto proporciona al negocio de la seguridad de la efectividad del control para satisfacer los requisitos relativos al negocio y a las responsabilidades sociales y regulatorias.			Evidencia de la efectividad de los controles de seguridad de la información	Interno

Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)
1. Medir la eficacia de los controles de seguridad de la información.
2. Realizar revisiones regulares de aplicaciones, sistemas y redes.

MEA02 Prácticas de Seguridad Específicos del Proceso, Entradas/Salidas y Actividades *(cont.)*				
	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas Especificas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
MEA02.03 Realizar autoevaluación de control. Estimular a la Dirección y a los propietarios de los procesos a tomar posesión de manera firme del procedimiento de mejora del control, a través de programas continuos de autoevaluación que valoren la completitud y efectividad del control de la Dirección sobre los procesos, políticas y contratos.	MEA02.01	Alcance para el aseguramiento de seguridad de la información y estrategia de evaluación de controles internos definidos	Evaluaciones de aseguramiento de seguridad de la información	MEA02.04
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Realizar evaluaciones del aseguramiento de seguridad de la información (independientes y auto-evaluaciones) para identificar debilidades de los controles.				
	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas Especificas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
MEA02.04 Identificar y comunicar las deficiencias de control Identificar deficiencias de control y analizar e identificar las causas raíces subyacentes. Escalar las deficiencias de control y comunicarlas a las partes interesadas.	MEA02.03	Evaluaciones de aseguramiento de seguridad de la información	Resultados de la evaluación y acciones de remedio	MEA02.08
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Revisar los informes de incidentes de seguridad de la información para identificar deficiencias de los controles. Informar y abordar las deficiencias detectadas.				
	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas Especificas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
MEA02.05 Garantizar que los proveedores de aseguramientos sean independientes y cualificados. Asegurar que las entidades que realizan el aseguramiento sean independientes de la función, grupo u organización en el alcance. Las entidades que realizan el aseguramiento deberían demostrar una actitud y apariencia apropiadas y adecuada competencia en las habilidades y conocimientos que son necesarios para realizar el aseguramiento y la adherencia a los códigos de ética y los estándares profesionales.			Competencias en habilidades y conocimiento	Interno
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Establecer competencias y cualificaciones para el proveedor de aseguramiento.				
	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas Especificas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
MEA02.06 Planificar iniciativas de aseguramiento. Planificar las iniciativas de aseguramiento basándose en los objetivos empresariales y las prioridades estratégicas, riesgo inherente, restricciones de recursos y suficiente conocimiento de la compañía.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Plan de compromiso	Plan de compromiso actualizado	Interno
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Aceptar los objetivos de la revisión de aseguramiento de seguridad de la información.				
	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas Especificas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
MEA02.07 Estudiar las iniciativas de aseguramiento. Definir y acordar con la dirección el ámbito de la iniciativa de aseguramiento, basándose en los objetivos de aseguramiento.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Plan de compromiso	Plan de compromiso actualizado	Interno
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Documentar los detalles del compromiso de la organización en completar la revisión.				

MEA02 Prácticas de Seguridad Específicos del Proceso, Entradas/Salidas y Actividades *(cont.)*				
	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas Especificas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
MEA02.08 Ejecutar las iniciativas de aseguramiento. Ejecutar la iniciativa de aseguramiento planificada. Informar de los hallazgos identificados. Proveer opiniones de aseguramiento positivo, cuando sea oportuno, y recomendaciones de mejora relativas a los riesgos residuales identificados en el desempeño operacional, el cumplimiento externo y el sistema de control interno.	DSS05.02	Resultados de pruebas de intrusión	Informes y recomendaciones de auditorías externas de seguridad de la información	Interno
	MEA02.04	Resultados de la evaluación y acciones de remedio		
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Producir y emitir informes firmados sobre el aseguramiento de seguridad de la información.				

Para más información relativa a los catalizadores relacionados, por favor consulte:
- Apéndice A. Guía Detallada: Catalizador de Principios, Políticas y Marcos de Referencia
- Apéndice F: Guía Detallada: Servicios, Infraestructura y Aplicaciones, F.10 Proporcionar Servicios de Monitorización y Alerta para Eventos de Seguridad
- Apéndice G: Guía Detallada: Personas, Habilidades y Competencias, G.6. Evaluación de la Información y Pruebas y Cumplimiento

Página dejada en blanco intencionadamente

MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	Área: Gestión Dominio: Supervisar, Evaluar y Valorar
Descripción del Proceso COBIT 5 Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general.	
Declaración del Propósito del Proceso COBIT 5 Asegurar que la empresa cumple con todos los requisitos externos que le sean aplicables.	

MEA03 Objetivos y Métricas de Seguridad Específicos del Proceso	
Objetivos de Seguridad Específicos del Proceso	**Métricas Relacionadas**
1. Las prácticas de riesgos y seguridad de la información conformes con los requerimientos de cumplimiento de externos.	• Porcentaje de prácticas de seguridad de la información que satisfacen los requerimientos externos de conformidad
2. Se realiza una supervisión de los requisitos externos nuevos o revisados que impactan en la seguridad de la información.	• Número o porcentaje de proyectos iniciados por seguridad de la información para implementar nuevos requerimientos externos

MEA03 Prácticas de Seguridad Específicos del Proceso, Entradas/Salidas y Actividades

Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas Específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
MEA03.01 Identificar requisitos externos de cumplimiento. Identificar y supervisar, de manera continuada, cambios en las legislaciones y regulaciones tanto locales como internacionales, así como otros requisitos externos de obligado cumplimiento en el área de TI.	BAI02.01	Requerimientos de seguridad de la información	Requerimientos externos de cumplimiento de seguridad de la información	BAI02.01
	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Estándares y regulaciones de seguridad de la información		
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Establecer acuerdos para supervisar la conformidad de seguridad de la información con requerimientos externos.				
2. Identificar objetivos de cumplimiento de seguridad de la información con requerimientos externos.				
3. Determinar los requerimientos externos de cumplimiento que deben satisfacerse (incluyendo legales, regulatorios, de privacidad y contractuales).				
4. Identificar y comunicar las fuentes de materiales relativos a seguridad de la información que ayuden a cumplir los requerimientos de cumplimiento externos.				

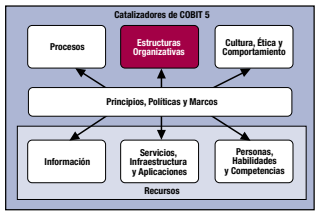
Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas Específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
MEA03.02 Optimizar la respuesta a requisitos externos. Revisar y ajustar políticas, principios, estándares, procedimientos y metodologías para asegurar la adecuada gestión y comunicación de los requisitos legales, regulatorios y contractuales. Considerar qué estándares sectoriales, códigos de buenas prácticas y guías de mejores prácticas pueden adoptarse y adaptarse.	Fuera del ámbito de *COBIT 5 para Seguridad de la Información*	Regulaciones aplicables	Requerimientos externos actualizados	Interno
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Revisar y comunicar los requerimientos externos a todos los grupos de interés relevantes.				

Práctica de Gestión	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		Salidas Específicas de Seguridad (Adicionales a las Salidas de COBIT 5)	
	De	**Descripción**	**Descripción**	**A**
MEA03.03 Confirmar el cumplimiento de requisitos externos. Confirmar el cumplimiento de las políticas, los principios, los estándares, los procedimientos y las metodologías con los requisitos legales, regulatorios y contractuales.			Informe de conformidad de seguridad de la información	Interno
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Recopilar y analizar los datos de conformidad relacionados con la gestión de la seguridad y de los riesgos de la información.				

MEA03 Prácticas de Seguridad Específicos del Proceso, Entradas/Salidas y Actividades *(cont.)*				
	Entradas específicas de seguridad (Adicionales a las Entradas COBIT 5)		**Salidas Específicas de Seguridad (Adicionales a las Salidas de COBIT 5)**	
Práctica de Gestión	**De**	**Descripción**	**Descripción**	**A**
MEA03.04 Obtener garantía del cumplimiento de requisitos externos. Obtener y notificar garantías de cumplimiento y adherencia a políticas, principios, estándares, procedimientos y metodologías. Confirmar que las acciones correctivas para tratar las diferencias en el cumplimiento son cerradas a tiempo.			Informes de aseguramiento de la conformidad	Interno
Actividades Específicas de Seguridad (Adicionales a las Actividades de COBIT 5)				
1. Obtener evidencias de las terceras partes.				

Para más información relativa a los catalizadores relacionados, por favor consulte:
- Apéndice A. Guía Detallada: Catalizador de Principios, Políticas y Marcos s de Referencia
- Apéndice F: Guía Detallada: Servicios, Infraestructura y Aplicaciones, F.10 Proporcionar Servicios de Monitorización y Alerta para Eventos de Seguridad
- Apéndice G: Guía Detallada: Personas, Habilidades y Competencias, G.6. Evaluación de la Información y Pruebas y Cumplimiento

Apéndice C
Guía Detallada: Catalizador de Estructuras Organizativas



Este apéndice trata del uso y la optimización de las entidades clave de toma de decisión sobre seguridad de la información en una empresa, sobre la base de la introducción del catalizador estructuras organizativas en la sección II:
- CISO (como se define en el marco de COBIT 5)
- ISSC
- ISM (como se define en el marco de COBIT 5)
- Comité de ERM
- Custodios de la Información/propietarios del negocio

Se proporcionan descripciones detalladas de estos grupos y roles, incluyendo:
- **Composición**—Debe requerirse un conjunto apropiado de habilidades a todos los miembros del grupo organizativo.
- **Mandato, principios operativos, ámbito de control y nivel de autoridad**—Estos elementos describen los acuerdos prácticos de cómo operará la estructura, los límites de los derechos de decisión de la estructura organizativa, las responsabilidades (tanto lo que ha de hacer, cómo de lo que es responsable de que se haga), y el escalado o acciones requeridas en caso de problemas.
- **Matriz RACI de alto nivel**—Las matrices RACI unen las actividades de proceso con las estructuras organizativas y/o los roles individuales en la empresa. Describen el nivel de implicación de cada rol para cada práctica del proceso: (A) Responsable de que se haga, (R) Responsable de hacerlo, (C) Consultado e (I) Informado.
- **Entradas/Salidas**—Una estructura requiere entradas (normalmente información) antes de que se puedan tomar decisiones informadas, y produce salidas tales como decisiones, otra información o peticiones de información adicional.

C.1 Director de Seguridad de la Información (CISO)

Mandato, Principios Operativos, Ámbito de Control y Nivel de Autoridad

La **figura 25** lista las características del CISO.

Figura 25—CISO: Mandato, Principios Operativos, Ámbito de Control y Nivel de Autoridad

Área	Característica
Mandato	La responsabilidad completa del programa de seguridad de la información de la empresa.
Principios operativos	Dependiendo de los factores variables en una empresa, el CISO puede reportar al CEO, COO, CIO, CRO o a otro ejecutivo sénior. El CISO es el enlace entre la dirección ejecutiva y el programa de seguridad de la información. El CISO debe también comunicar y coordinarse de manera muy cercana con los grupos de interés clave del negocio para cubrir las necesidades de protección de la información. El CISO debe: • Tener un entendimiento exacto de la visión estratégica del negocio • Ser un comunicador efectivo • Ser hábil en construir relaciones efectivas con los líderes del negocio • Ser capaz de traducir los objetivos del negocio en requerimientos de seguridad de la información
Ámbito de control	El CISO es responsable de: • Establecer y mantener un sistema de gestión de seguridad de la información (SGSI) • Definir y gestionar un plan de tratamiento del riesgo de la información • Supervisar y revisar el SGSI

Nivel de autoridad/derechos de decisión	El CISO es responsable de implementar y mantener la estrategia de seguridad de la información. La responsabilidad de que se haga (y la aprobación de las decisiones importantes) reside en la función a la que el CISO reporta, por ejemplo, un miembro de la directiva ejecutiva sénior o el ISSC.
Derechos de delegación	El CISO debe delegar las tareas a los gerentes de seguridad de la información y a personal de negocio.
Escalado	El CISO debe escalar problemas clave relacionados con el riesgo de información a su supervisor directo y/o al ISSC.

Matriz RACI a Alto Nivel

La matriz RACI en la **figura 26** está limitada a ejemplos importantes de prácticas claves para las cuales el CISO debe ser responsable de que se hagan o realizarlas.

Figura 26—CISO: Matriz RACI a Alto Nivel con Prácticas Clave

Práctica de Proceso	Nivel de Implicación (RACI)
Identificar y comunicar amenazas para la seguridad de la información, comportamientos deseables y cambios necesarios para tratar estos puntos.	Responsable de que se haga
Asegurar que la gestión del entorno y de las instalaciones se adhiere a los requerimientos en seguridad de la información.	Responsable de que se haga
Protección contra malware.	Responsable de que se haga
Gestionar la seguridad de las redes y la conectividad.	Responsable de que se haga
Gestionar la seguridad del perímetro.	Responsable de que se haga
Gestionar la identidad de los usuarios y el acceso lógico.	Responsable de que se haga
Gestionar el acceso físico a los activos de TI.	Responsable de que se haga
Supervisar la infraestructura para identificar eventos relacionados con la seguridad.	Responsable de que se haga
Proporcionar formas de mejorar la eficiencia y la eficacia de la función de seguridad de la información (por ejemplo, mediante formación del personal de seguridad de la información; documentación de procesos, tecnología y aplicaciones; y la estandarización y automatización del proceso).	Responsable de que se haga
Supervisar la gestión del riesgo en TI.	Responsable de hacerla
Definir y comunicar la estrategia en seguridad de la información que está alineada con la estrategia del negocio.	Responsable de hacerla
Investigar, definir y documentar los requerimientos en seguridad de la información.	Responsable de hacerla
Validar los requerimientos en seguridad de la información con las partes interesadas, patrocinadores del negocio y personal de despliegue técnico.	Responsable de hacerla
Desarrollar políticas y procedimientos de seguridad de la información.	Responsable de hacerla
Definir e implementarestrategias de evaluación del riesgo y de respuesta y cooperar con la oficina del riesgo para gestionar el riesgo de la información.	Responsable de hacerla
Asegurar que se evalúa el impacto potencial de los cambios.	Responsable de hacerla
Recoger y analizar datos del rendimiento y de cumplimiento relativos a seguridad de la información y gestión del riesgo de la información.	Responsable de hacerla

Entradas/Salidas

Una estructura requiere entradas (normalmente información) antes de que se puedan tomar decisiones informadas, y produce salidas tales como decisiones, otra información o peticiones de información adicional. La **figura 27** contiene una lista no exhaustiva de tales entradas y salidas.[5]

Figura 27—CISO: Entradas y Salidas

Entrada	De	Salida	A
Tolerancia al riesgo	ERM	Estrategia de seguridad de la información	Comité de ERM
Mandato regulatorio/de cumplimiento	Externo	Políticas, estándares, procedimientos	Empresa
Estrategia de negocio y de TI	Organización/TI	Plan de remediación a las recomendaciones de auditoría	Auditoría
Informes de auditoría	Auditoría		

[5] Estas entradas y salidas no deben confundirse con las entradas y salidas de proceso como se describe en la sección II. Sin embargo, en algunos casos, las entradas y salidas de una estructura organizativa son información entregada por un proceso, en cuyo caso, son salidas de proceso.

C.2 Comité de Dirección de Seguridad de la Información

Composición

La **figura 28** describe los roles de los miembros del ISSC.

Figura 28—ISSC: Composición	
Rol	**Descripción**
CISO	• Presidir el ISSC y ser el enlace con el Comité de ERM • Responsable de toda la seguridad de la información de la empresa
ISM	Comunicación de las prácticas de diseño, implementación y monitorización Cuando sea aplicable, el ISM discute las soluciones de diseño por adelantado con los arquitectos de seguridad de la información para mitigar los riesgos de la información identificados.
Custodios de la información/ propietarios del negocio	• A cargo de ciertos procesos o aplicaciones de negocio • Responsables de comunicar tanto iniciativas de negocio que puedan impactar en la seguridad de la información como el impacto que las prácticas de seguridad de la información puedan causar a los usuarios • Pueden tener una comprensión del riesgo de negocio/operativo, costes y beneficios, así como de determinados requerimientos de seguridad de la información para su área de negocio
Gerente de TI	Informar del estado de las iniciativas de seguridad de la información relacionadas con TI
Representantes de las funciones especializadas	Aportar la opinión de los especialistas al comité cuando sea relevante, por ejemplo, de representantes de auditoría interna, RRHH, legal, riesgo, oficial de gestión de proyectos (PMO). A estas funciones se les puede pedir que se unan al ISSC en ocasiones o como miembros permanentes. Puede merecer la pena tener representantes de auditoría interna como miembros permanentes para dar consejo al comité sobre el riesgo de cumplimiento.

Mandato, Principios Operativos, Ámbito de Control y Nivel de Autoridad

La **figura 29** describe las características del ISSC.

Figura 29—ISSC: Mandato, Principios Operativos, Ámbito de Control y Nivel de Autoridad	
Área	**Característica**
Mandato	Asegurar que las buenas prácticas, que la seguridad de la información se aplican de forma eficaz y consistentemente en toda la empresa.
Principios operativos	• El ISSC se reúne de manera regular, cuando sea necesario para la empresa. Se pueden planificar reuniones más frecuentes durante iniciativas específicas o cuando haya problemas que necesiten ser gestionados urgentemente. • Se permiten sustitutos o representantes, pero deben limitarse. • Se debe limitar la pertenencia al comité a un número pequeño de líderes estratégicos y tácticos para asegurar la comunicación bidireccional y la toma de decisiones adecuadas. Otros líderes de negocio pueden ser invitados según la necesidad. • Todas las actas de las reuniones deben ser aprobadas y retenidas por un determinado periodo de tiempo. • El CISO preside las reuniones del ISSC.
Ámbito de control	El ISSC es responsable en la toma de decisiones de seguridad de la información para toda la empresa.
Nivel de autoridad/derechos de decisión	El ISSC es responsable de las decisiones de seguridad de la información de la empresa en apoyo a las decisiones estratégicas del comité de ERM.
Derechos de delegación	El ISSC es el último responsable de la estrategia de diseño e implementación del programa de seguridad de la información y esta responsabilidad no se puede delegar a otros roles miembros.
Escalado	Todos los problemas deben ser escalados al miembro responsable de seguridad de la información pertinente de la dirección ejecutiva. Las estrategias del riesgo de la información de la empresa deben ser escaladas para su aprobación al comité de ERM.

Matriz RACI a Alto Nivel

La **figura 30** describe el nivel de implicación del ISSC.

Figura 30—ISSC: Matriz RACI a Alto Nivel	
Práctica de Proceso	**Nivel de Implicación (RACI)**
Definir y comunicar la estrategia de seguridad de la información que está alineada con la estrategia del negocio.	Responsable de que se haga
Investigar, definir y documentar los requerimientos en seguridad de la información.	Responsable de que se haga
Validar los requerimientos en seguridad de la información con las partes interesadas, patrocinadores del negocio y personal de despliegue técnico.	Responsable de que se haga
Desarrollar políticas y procedimientos de seguridad de la información.	Responsable de que se haga
Desarrollar un plan de seguridad de la información que identifique el entorno de seguridad de la información y las actividades a ser implementadas por el equipo de proyecto para proteger los activos de la organización.	Responsable de que se haga
Asegurar que se evalúa el impacto potencial de los cambios.	Responsable de que se haga
Recoger y analizar datos del rendimiento y de cumplimiento relativos a seguridad de la información y gestión del riesgo de la información.	Responsable de que se haga
Establecer, acordar y comunicar el rol del CISO y el ISM.	Responsable de hacerla
Aumentar el perfil de la función de seguridad de la información dentro de la empresa y potencialmente fuera de ella.	Responsable de hacerla
Contribuir al esfuerzo en la gestión de la continuidad de negocio de toda la empresa.	Responsable de hacerla

Entradas/Salidas

Una estructura requiere entradas (normalmente información) antes de que se puedan tomar decisiones informadas, y produce salidas tales como decisiones, otra información o peticiones de información adicional. La **figura 31** contiene una lista no exhaustiva de tales entradas y salidas.[6]

Figura 31—ISSC: Entradas y Salidas			
Entrada	**De**	**Salida**	**A**
Estrategia de negocio	Consejo de Administración	Programa y estrategia de seguridad de la información	Comité de ERM, ISMs, custodios de la Información/dueños del negocio
Niveles de aceptación del riesgo	Comité de ERM	Perfil del riesgo de la información	Comité de ERM
Estrategia de TI	TI		
Listado de proyectos de la empresa	Custodios de la información/ propietarios del negocio, PMO		
Informes de auditoría interna	Auditoría interna		

C.3 Gerente de Seguridad de la Información (ISM)

Mandato, Principios Operativos, Ámbito de Control y Nivel de Autoridad

La **figura 32** presenta las características del ISM.

Figura 32—ISM: Mandato, Principios Operativos, Ámbito de Control y Nivel de Autoridad	
Área	**Característica**
Mandato	Responsabilidad completa de la gestión de los esfuerzos en seguridad de la información
Principios operativos	Informa al CISO (o, en algunas empresas, a los líderes de las unidades de negocio)
Ámbito de control	Seguridad de la información en aplicaciones, en infraestructuras, gestión de accesos, gestión de amenazas e incidentes, gestión del riesgo, programa de concienciación, métricas, evaluación de proveedores
Nivel de autoridad/derechos de decisión	Autoridad completa en la toma de decisiones sobre las prácticas del dominio de la seguridad de la información
Derechos de delegación	No debe delegar las decisiones relacionadas con las prácticas del dominio de la seguridad de la información
Escalado	Escalar problemas al CISO

[6] Estas entradas y salidas no deben confundirse con las entradas y salidas de procesos descritas en la sección II. Sin embargo, en algunos casos, las entradas y salidas de estructuras organizativas son informaciones proporcionadas por un proceso, en cuyo caso se consideran salidas de procesos.

Matriz RACI de Alto Nivel

La **figura 33** muestra el nivel de implicación del ISM.

Figura 33—ISM: Matriz RACI de Alto Nivel	
Práctica del Proceso	**Nivel de Implicación (RACI)**
Desarrollar y comunicar una visión común al equipo de seguridad de la información que esté en línea con la declaración de visión corporativa.	Responsable de hacerla
Gestionar la asignación de personal de seguridad de la información de acuerdo con las necesidades del negocio.	Responsable de hacerla
Realizar evaluaciones de riesgos de la información y definir el perfil de riesgo de la información.	Responsable de hacerla
Gestionar roles, responsabilidades, privilegios de accesos y niveles de autoridad.	Responsable de hacerla
Desarrollar un plan de seguridad de la información que identifique el entorno de seguridad de la información y los controles que deben ser implementados por el equipo del proyecto para proteger los activos de la organización. Supervisar estos controles internos y ajustarlos/mejorarlos cuando sea necesario.	Responsable de hacerla
Identificar y comunicar los puntos débiles de la seguridad de la información, los comportamientos deseables y los cambios necesarios para hacer frente a estas debilidades.	Responsable de hacerla
Proporcionar formas de mejorar la eficiencia y la eficacia de la función de seguridad de la información (por ejemplo,mediante formación del personal de seguridad de la información; documentación de procesos, tecnología y aplicaciones; y la estandarización y automatización del proceso).	Responsable de hacerla
Recoger y analizar datos del rendimiento y de cumplimiento relativos a seguridad de la información y gestión del riesgo de la información.	Responsable de hacerla
Asegurar que la gestión del entorno y de las instalaciones se adhiere a los requerimientos en seguridad de la información.	Responsable de hacerla

Entradas/Salidas

Una estructura requiere entradas (normalmente información) antes de que se puedan tomar decisiones informadas, y produce salidas tales como decisiones, otra información, o peticiones de información adicional. La **figura 34** contiene una lista no exhaustiva de tales entradas y salidas.[7]

Figura 34—ISM: Entradas y Salidas			
Entrada	**De**	**Salida**	**A**
Estrategia de seguridad de la información	ISSC	Diseño, implementación y planes de mejora para las prácticas de seguridad de la información	Empresa
Planificación/arquitectura/ configuraciones de infraestructura de TI	TI	Evaluaciones periódicas de riesgos de la información y pruebas de las prácticas de seguridad de la información y de contramedidas	CISO, Líneas de negocio
Políticas/estándares/ procedimientos de seguridad de la información	CISO/ISM	Informes de situación de la implementación de la seguridad de la información	CISO
Tolerancia al riesgo	ERM		
Mandato regulatorio/de cumplimiento	Externo		
Estrategia de negocio y de TI	Organización/TI		
Informes de auditoría	Auditoría		

[7] Estas entradas y salidas no deben confundirse con las entradas y salidas de procesos descritas en la sección II. Sin embargo, en algunos casos, las entradas y salidas de estructuras organizativas son informaciones proporcionadas por un proceso, en cuyo caso se consideran salidas de procesos.

C.4 Comité de Gestión de Riesgo Empresarial

El comité de ERM es responsable de todas la toma de decisiones de la empresa relativas a la evaluación, control, optimización, financiación y monitorización de todas las fuentes de riesgo, con el propósito de incrementar el valor de la empresa a corto y largo plazo para todas sus partes interesadas.

Composición

La **figura 35** muestra los roles de los miembros del comité de ERM.

Figura 35—Comité de ERM: Composición	
Rol	**Descripción**
CISO	En un escenario óptimo, el CISO es miembro del comité de ERM, para proporcionar al comité asesoramiento sobre riesgos específicos de la información.
CEO, COO, CFO, etc.	Representante de la alta dirección ejecutiva.
Propietarios de los procesos clave para el negocio	• A cargo de ciertos procesos o aplicaciones de negocio • Responsables de comunicar tanto iniciativas de negocio que puedan impactar en la seguridad de la información como el impacto que las prácticas de seguridad de la información puedan causar a los usuarios • Pueden tener una comprensión del riesgo de negocio/operativo, costes y beneficios, así como de determinados requerimientos de seguridad de la información para su área de negocio
Auditoría/ cumplimiento	Proporciona información especializada cuando sea relevante. Se les puede pedir su incorporación al comité de ERM de manera ocasional o como miembro permanente. Por ejemplo, puede merecer la pena tener representantes de la auditoría interna como miembros permanentes con objeto de asesorar al comité en materia de riesgo de cumplimiento.
Representante legal	Proporciona asesoramiento legal. Se le puede pedir su incorporación al comité de ERM de manera ocasional o como miembro permanente.
CRO	Proporciona información especializada cuando sea relevante. Se le puede solicitar su incorporación al comité de ERM de manera ocasional o como miembro permanente.

Matriz RACI de Alto Nivel

La **figura 36** muestra el nivel de implicación de los miembros del comité de ERM.

Figura 36—Comité de ERM: Matriz RACI de Alto Nivel	
Práctica del Proceso	**Nivel de Implicación (RACI)**
Asesorar sobre la estrategia de seguridad de la información definida por el ISSC.	Responsable de hacerla
Establecer los niveles de tolerancia al riesgo de la empresa.	Responsable de que se haga
Definir e implementar las estrategias de evaluación y de respuesta al riesgo.	Responsable de que se haga
Revisar las evaluaciones de riesgos de la información y los perfiles de riesgos.	Responsable de que se haga

C.5 Custodios de la Información/Propietarios de Negocio

Composición

Los custodios de la información o los propietarios de negocio actúan como enlaces entre las funciones de negocio y de seguridad de la información. Pueden ser asociados con tipos de información, aplicaciones específicas, o unidades de negocio dentro de una empresa. La persona que desempeñe este rol debe poseer un buen conocimiento tanto del negocio como de los tipos de información que son procesados y que requieren protección. Actúan como asesores de confianza y agentes de supervisión en cuestiones relativas a la información dentro del negocio.

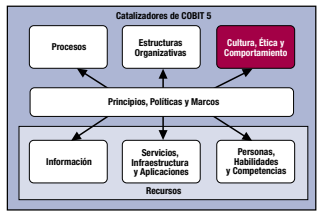
Este rol debería equilibrar el riesgo de negocio y el de información de modo que las decisiones del negocio no prevalezcan siempre sobre las decisiones de la seguridad de la información.

Matriz RACI de Alto Nivel

La **figura 37** muestra el nivel de implicación de los custodios de información y propietarios de negocio.

Figura 37—Custodios de la Información/Propietarios de Negocio: Matriz RACI de Alto Nivel	
Práctica del Proceso	**Nivel de Implicación (RACI)**
Comunicar, coordinar y asesorar a los gestores de negocio sobre los esfuerzos en gestión de riesgos de la información.	Responsable de hacerla
Informar al ISSC sobre cambios en los procesos de negocio y/o en las estrategias (por ejemplo, nuevos productos o servicios).	Responsable de hacerla
Elevar el perfil de la función de seguridad de la información y de las políticas y procedimientos de seguridad de la información dentro de la empresa.	Responsable de hacerla

Apéndice D
Guía Detallada: Catalizador de Cultura, Ética y Comportamiento



Este apéndice proporciona detalles sobre los comportamientos de seguridad de la información tal y como se presentan en la sección II. Se pueden identificar ocho comportamientos deseables en relación a la seguridad de la información (comentados en la parte restante del apéndice) que influirán positivamente tanto en la cultura sobre seguridad de la información como en su implementación práctica en el día a día de la empresa.

Para cada uno de los comportamientos definidos se describen en este apéndice los atributos siguientes:
- **Ética organizativa**—Determinada por los valores con los que la empresa se quiere identificar.
- **Éticas individuales**—Determinadas por los valores personales de cada individuo dentro de la empresa y dependiendo en un importante grado de factores externos tales como creencias, origen étnico, antecedentes socioeconómicos, ubicación geográfica y experiencias personales.
- **Liderazgo**—Maneras en que el liderazgo puede influir en comportamientos apropiados:
  – Cómo la comunicación y la aplicación de normas y reglas puede ser utilizada para influir en el comportamiento.
  – - Incentivos y recompensas que pueden utilizarse para influir en el comportamiento.
  – Mejora de la concienciación.

D.1 Comportamientos

Cada uno de los comportamientos siguientes está presente en las empresas en dos niveles: el **nivel organizativo**, en el que los comportamientos están determinados por los valores (éticos, culturales o actitudes) con los que la empresa se quiere identificar, y el **nivel individual** en el que los comportamientos se definen por valores personales (éticos, culturales o actitudes).

Comportamiento 1: La seguridad de la información se practica en las operaciones diarias.
La seguridad de la información es parte del funcionamiento diario de la empresa. A nivel organizativo, el comportamiento indica que la seguridad de la información se acepta como un imperativo empresarial en el establecimiento de los objetivos organizativos. A nivel individual, esto significa que a los individuos les importa el bienestar de la empresa y por lo tanto aplican técnicas de seguridad de la información y un enfoque de prudencia en sus operaciones cotidianas.

Comportamiento 2: Las personas respetan la importancia de las políticas y principios de la seguridad de la información.
El personal de la empresa reconoce la importancia de las políticas y principios de la seguridad de la información. A nivel organizativo, la alta dirección respalda las políticas y principios aprobándolas, revisándolas y comunicándolas de manera regular. A nivel individual, los empleados han leído y comprendido las políticas, y se sienten capacitados para seguir las directivas de la empresa.

Comportamiento 3: Las personas poseen un nivel detallado y suficiente de orientación en seguridad de la información y se les anima a participar y cuestionar la situación actual de seguridad de la información.
Las personas poseen un nivel detallado y suficiente de orientación en seguridad de la información y se les anima a participar y cuestionar la situación actual de seguridad de la información en dos niveles. La cultura organizativa indica un proceso de comunicación de dos vías para la orientación y para la retroalimentación y proporciona a las partes interesadas una oportunidad para realizar comentarios sobre los cambios; la cultura individual demuestra la participación de las partes interesadas cuestionando y proporcionando comentarios cuando se les solicita.

Comportamiento 4: Todo el personal es responsable de que se proteja la información de la empresa.
Esta responsabilidad se refleja en dos niveles dentro de la empresa. En el nivel organizativo, se hacen constar aquellas incidencias que impliquen responsabilidades (disciplina), y se confirman los roles de las partes interesadas relativos a su aplicación. En el nivel individual se requiere a cada individuo que comprenda las responsabilidades asumidas relativas a la seguridad de la información.

Comportamiento 5: Las Partes Interesadas están informadas de cómo identificar y responder a las amenazas en el contexto de la empresa.
Se pueden implementar los procesos adecuados para identificar y responder a las amenazas a nivel organizativo mediante la instauración de un proceso de notificación de incidencias y de un proceso para minimizar las pérdidas de información. A nivel individual, el personal debe estar formado sobre qué constituye un incidente de seguridad, cómo se debe notificar sobre él y cómo reaccionar.

Comportamiento 6: La Dirección respalda y anticipa las innovaciones en seguridad de la información de manera proactiva y lo comunica a toda la empresa. La empresa es receptiva para tener en cuenta y manejar nuevos retos en materia de seguridad de la información.

Las innovaciones y retos en seguridad de la información se abordan a nivel organizativo mediante un equipo de investigación y desarrollo en seguridad de la información. La cultura individual contribuye con las partes interesadas para aportar nuevas ideas.

Comportamiento 7: La Dirección de negocio se compromete a colaborar transversalmente de manera continuada para conseguir programas de seguridad de la información efectivos y eficientes.

La colaboración multifuncional se alcanza mediante la aceptación por parte de la organización de una estrategia de seguridad de la información con un enfoque holístico y a través de una integración mejorada con el negocio. Los individuos contribuyen a través del acercamiento a otras funciones de negocio y mediante la identificación de posibles sinergias.

Comportamiento 8: La alta dirección reconoce el valor para el negocio de la seguridad de la información.

El valor para el negocio de la seguridad de la información se reconoce a nivel organizativo en cuanto la seguridad de la información se ve como un medio para mejorar el valor del negocio (beneficio, coste, reputación y ventaja competitiva), la transparencia en la respuesta a las incidencias es clave y se considera esencial comprender las expectativas de los clientes. A nivel individual, este comportamiento se pone de manifiesto con la generación de ideas creativas que generan valor (a varios niveles dentro de la seguridad de la información).

D.2 Liderazgo

Los comportamientos que se acaban de describir pueden ser influidos por el liderazgo a diferentes niveles de la empresa, como se esbozó en la sección II, subsección 5.3. Se pueden distinguir tres niveles de liderazgo: la gerencia de seguridad de la información (CISO/ISM) en el nivel de seguridad de la información, la gerencia del negocio en el nivel de la unidad de negocio y la alta dirección en el nivel más alto. Estos niveles de liderazgo influyen en el comportamiento mediante la utilización de comunicaciones, disposiciones, normas, implantación de incentivos y recompensas, así como labores de concienciación.

Influenciando en el Comportamiento Mediante Comunicaciones, Disposiciones, Reglas y Normas.

El liderazgo utiliza comunicaciones, disposiciones, reglas y normas con objeto de influir en los comportamientos dentro de la empresa. La comunicación es siempre esencial para influir en cualquier tipo de comportamiento. La aplicación de una cultura de seguridad de la información es dependiente del grado de importancia de este aspecto dentro de la cultura. Las normas pueden utilizarse para forzar acciones internas cuando la seguridad de la información es obligatoria desde el punto de vista legal.

La gerencia de seguridad de la información (CISO/ISM) se ocupa de que la seguridad de la información esté incorporada en las políticas y procedimientos y de que se realicen acciones de orientación y de puesta al día. Además, el CISO/ISM realiza una recertificación anual de las políticas y principios. Junto a la **alta dirección**, el CISO/ISM realiza un acuerdo formal de estas políticas. Los gerentes de las unidades de negocio dan seguimiento a las acciones correctivas y la alta dirección realiza una revisión anual del rendimiento de la seguridad de la información.

El **CISO/ISM** trabaja junto a los **gerentes de las unidades de negocio** para asegurar la aprobación de las partes interesadas. Los gerentes de las unidades de negocio constituyen un ejemplo para el resto a través de su liderazgo. El CISO/ISM implementa un proceso de notificación de incidencias, apoyado por un mecanismo de generación de informes que incluye disparadores para alertar a las partes interesadas (clientes, proveedores, etc.). El CISO/ISM se encarga también de seguir las tendencias del mercado, tanto en cuestiones de seguridad de la información como de negocio.

Mientras que la **alta dirección** se asegura de que la seguridad de la información esté correctamente representada en las estructuras correctas (comités, grupos de trabajo, equipos de implementación), el **CISO/ISM** comunica los procesos de seguridad de la información a toda la empresa.

Influyendo en el Comportamiento Mediante Incentivos y Recompensas

La Dirección influye en el comportamiento empleando medidas diseñadas para proporcionar un refuerzo positivo para las conductas deseables y un refuerzo negativo para las conductas desaconsejables. La ausencia de recompensas inhibe la adopción de una cultura de seguridad de la información. La gerencia del negocio necesita saber que los comportamientos seguros serán recompensados; este aspecto implica que la alta dirección debe dejar claras sus intenciones favoreciendo la implantación de salvaguardas de seguridad y promoviendo actitudes ejemplares de cultura de seguridad. Estas recompensas no implican pagos monetarios directos a los individuos; en su lugar, pueden constituir mejoras organizativas en forma de presupuestos, influencias, atención de la dirección, etc. Aunque algunas personas sólo están motivadas por la remuneración, otras aprecian otros tipos de reconocimiento.

Los siguientes incentivos y recompensas pueden ser utilizados por los distintos niveles de la gerencia para influir en el comportamiento:

La gerencia de seguridad de la información (CISO/ISM) puede organizar sesiones sobre la seguridad de la información en la vida privada (por ejemplo cubriendo la utilización de las redes sociales por los niños o la configuración de redes inalámbricas), con objeto de incorporar la seguridad de la información en la vida diaria, dar un reconocimiento positivo a los logros en materia de seguridad de la información, y distribuir complementos salariales por la innovación en seguridad de la información. El CISO/ISM no es el único nivel de gerencia que otorga estos complementos; la alta dirección puede también conceder recompensas por notificación de amenazas o por cualquier otra idea aprovechable.

La **gerencia del negocio** se focaliza en la seguridad de la información como un componente de la evaluación del rendimiento y asegura que figure en todas las descripciones de los puestos de trabajo, mientras que la **alta dirección** diseña incentivos y recompensas en función de la responsabilidad de las partes interesadas. **La gerencia del negocio** es responsable de realizar una revisión anual del programa de incentivos y recompensas y apoya la idea de que las políticas de seguridad son un requisito para la ocupación de un puesto de trabajo (cláusulas de los contratos laborales).

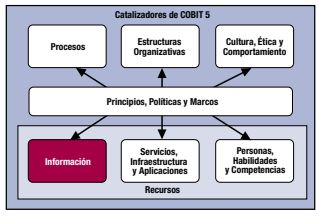
Influyendo en el Comportamiento Mediante la Mejora de la Concienciación

Los programas de concienciación tienen su función, pero no son suficientes por sí solos. El personal no necesita solamente ser concienciado de la importancia de la seguridad de la información sino que necesita ser formado en seguridad y en su rol personal dentro de ella. Los distintos niveles de gerencia dentro de una empresa pueden mejorar la concienciación a través de los medios siguientes.

La gerencia de seguridad de la información puede organizar acciones de formación en concienciación sobre materias de seguridad de la información, complementadas con sesiones periódicas de actualización, y asegurar que las políticas están siempre accesibles (por ejemplo a través de su publicación en Internet). El CISO/ISM es también responsable de compartir conocimientos en materia de amenazas, a través de una comunicación periódica de nuevas ideas y resultados, realizando un seguimiento de las tendencias del mercado y realizando análisis competitivos. **La gerencia del negocio** sigue habitualmente estas sesiones formativas y es responsable de la realización de notificaciones o peticiones de comentarios sobre los cambios propuestos. **La alta dirección** se encarga de que los incidentes de seguridad se notifiquen al personal.

Página dejada en blanco intencionadamente

Apéndice E
Guía Detallada: Catalizador de Información



Este apéndice proporciona detalles sobre el uso y optimización de los tipos de información relacionados con la seguridad de la información, basándose en la introducción del catalizador información de la sección II. Se proporciona un enfoque para mapear las partes interesadas involucradas en el uso de los diferentes tipos de información. Además, se listan todos los tipos de información, entre los que se encuentran:

- Estrategia de seguridad de la información
- Presupuesto de seguridad de la información
- Planificación de seguridad de la información
- Políticas
- Requerimientos de seguridad de la información, que podrían incluir:
  - Requisitos de configuración de la seguridad
  - Requisitos de seguridad de la información en los acuerdos a nivel de servicio (SLA) y en los acuerdos a nivel operacional (OLA)
- Material para la concienciación
- Informes de revisión de seguridad de la información, que podrían incluir:
  - Hallazgos de auditorías de seguridad de la información
  - Informes de madurez de seguridad de la información
  - Gestión de riesgos relacionada con la seguridad de la información:
    - Análisis de amenazas
    - Informes de evaluación de vulnerabilidades
- Catálogo de servicios de seguridad de la información
- Información sobre el perfil de riesgo, que incluye:
  - El registro de riesgos
  - Informes de violaciones y pérdidas (informe consolidado de incidentes)
- Cuadro de mando de seguridad de la información (o equivalentes), que incluye:
  - Incidentes de seguridad de la información
  - Problemas de seguridad de la información
  - Métricas de seguridad de la información

Para cada uno de los tipos de información, se proporciona una guía más detallada que incluye:

- **Metas**—Describe los objetivos que se deben alcanzar utilizando las tres categorías definidas en el modelo de información. Para estos tipos de información, los objetivos de información están divididos en tres dimensiones de calidad:
  - **Calidad intrínseca**—Indica el grado en que los valores de los datos cumplen con los valores reales o verdaderos
  - **Calidad contextual**—Indica el grado en que la información es aplicable a las tareas del usuario de la información y se presenta de una manera inteligible y clara de tal forma que se reconozca que la calidad de la información depende del contexto en que se use
  - **Calidad de la seguridad/accesibilidad**—Indica el grado en que la información está disponible o se puede obtener
- **Ciclo de vida**—Descripción específica de los requerimientos del ciclo de vida
- **Buenas prácticas del tipo de información**—Descripción de contenidos y estructura típicos

E.1 Plantilla para las Partes Interesadas de la Seguridad de la Información

En la **figura 38** se muestra una plantilla para mapear las partes interesadas con los tipos de información relacionados con seguridad de la información. Esta plantilla contiene:

- Descripción del grupo de interés o parte interesada: - Basada en la lista genérica de estructuras organizativas de COBIT 5 (también utilizada en la matriz RACI de las descripciones de proceso) y complementada con otras partes interesadas adicionales y externas para este dominio específico
- Tipos de información: Según se describe en el apéndice B. Guía Detallada: Catalizador de la Información

Es esencial identificar la parte interesada de la información para optimizar el desarrollo y la distribución de la información a lo largo de toda la empresa. La plantilla de la **figura 38** puede ayudar en el ejercicio de dicha identificación. La tabla debe ser adaptada al entorno específico traduciendo los ejemplos de tipos de información y las descripciones genéricas de las partes interesadas.

Se puede utilizar un indicador de la naturaleza de relación entre la parte interesada y cada tipo de información del tipo (ver el ejemplo de la **figura 17**):

- A—Aprobador
- O—Origen (emisor)
- I—Destino para fines de información
- U—Destino: usuario de la información

Figura 38—Plantilla de Información Relacionada con Partes Interesadas para la Seguridad de la Información

Parte Interesada	Tipo de información									
	Estrategia de Seguridad de la Información	Presupuesto de Seguridad de la Información	Plan de Seguridad de la Información	Políticas	Requerimientos de Seguridad de la Información	Material de Concienciación	Informes de Revisión de Seguridad de la Información	Catálogo de Servicios de Seguridad de la Información	Perfil de Riesgo de la Información	Cuadro de Mando de Seguridad de la Información
Interno: Empresa										
Consejo de Administración										
Director General Ejecutivo (CEO)										
Director General Financiero (CFO)										
Director General Operativo (COO)										
Director General de Riesgos (CRO)										
Comité de Dirección de la Seguridad de la Información (ISSC)										
Director de Seguridad de la Información (CISO)										
Ejecutivo de Negocio										
Propietario del proceso de negocio										
Comités de Supervisión (Proyecto y Programa)										
Comité de Arquitectura										
Comité de Gestión de riesgo empresarial (ERM)										
Jefe de Recursos Humanos (HR)										
Cumplimiento										
Auditoría										
Oficina de Gestión de Programas y Proyectos (PMO)										
Oficina de Gestión del Valor (VMO)										
Interno: TI										
Comité de Estrategia (Dirección de TI)										
Director Informática/Sistemas (CIO)										
Jefe de Arquitectura										
Jefe de Desarrollo										
Jefe de Operaciones de TI										
Jefe de Administración de TI										
Gerente de Servicios										
Gerente de Seguridad de la Información (ISM)										
Gerente de Continuidad de Negocio										
Oficial de Privacidad										
Externo										
Inversores										
Aseguradores										
Autoridades (aplicación de la ley)										
Reguladores										
Socios de Negocio										
Vendedores/Proveedores										
Auditores Externos										

E.2 Estrategia de Seguridad de la Información

Metas

La estrategia de la seguridad de la información debe esforzarse por estar a la vanguardia y en línea con principios generalmente reconocidos. Además, la arquitectura y el diseño deben estar alineados con la arquitectura empresarial y la situación específica de la organización, ser exhaustiva y completa y contener toda la información que se requiera con un nivel de detalle apropiado para su procesamiento. La estrategia de la seguridad de la información debe estar disponible solo para aquellos que necesitan dicho acceso (p. ej. partes interesadas).

Estas metas pueden medirse con métricas tales como:
- Porcentaje de actividades de la seguridad de la información que siguen un marco reconocido o comparable a las organizaciones similares
- Cantidad de divergencias entre la estrategia de la seguridad de la información y la arquitectura y la arquitectura de la empresa
- Porcentaje de partes interesadas sin acceso a la estrategia de seguridad de la información
- Cantidad de violaciones de seguridad de la información

Ciclo de Vida

Generalmente, una empresa define su estrategia y arquitectura a medio plazo para poder cumplir con la situación futura deseada, aunque permitiendo la realización de actualizaciones a corto plazo (p. ej. anualmente). Además, la estrategia de la seguridad de la información debe estar disponible para todas las partes interesadas relevantes.

Buena Práctica

El CISO/ISM es el responsable de desarrollar la estrategia de la seguridad de la información para la empresa. El propósito de la estrategia de la seguridad de la información es proporcionar a la empresa una dirección adecuada respecto a temas relativos a la seguridad de la información y que incluya a toda la empresa; por ejemplo alta dirección, auditorías, gerencia del negocio, desarrollo de TI y operaciones de TI.

El desarrollo de la estrategia de seguridad de la información se describe como sigue:

> *La estrategia de negocio proporciona una hoja de ruta para cumplir con los objetivos del negocio. Además, debe proporcionar una de las aportaciones principales a la estrategia de seguridad de la información. Este flujo sirve para promover el alineamiento de la seguridad de la información con los objetivos del negocio. Se llega al equilibrio de las aportaciones determinando el estado deseado de la seguridad [de la información] en contraposición al estado actual o existente. Los procesos de negocio deben también ser considerado, al igual que los riesgos principales de la organización, incluyendo los requerimientos regulatorios y el análisis de impacto asociado para determinar los niveles de protección y las prioridades.*
>
> *El objetivo de la estrategia de la seguridad [de la información] es el estado deseado definido por el negocio y los atributos de seguridad [de la información]. La estrategia proporciona las bases para un plan de acción que abarque uno o más programas de seguridad [de la información] que cuando se implementen alcancen los objetivos de la seguridad [de la información]. El plan o planes de acción deben de ser formulados basándose en los recursos disponibles y las limitaciones considerando a su vez los requerimientos regulatorios y legales relevantes.*
>
> *La estrategia y los planes de acción deben contener las condiciones para la supervisión, así como métricas definidas para determinar el nivel de éxito. El CISO y el Comité de Supervisión se retroalimentarán de esta información de tal forma que puedan hacer correcciones durante la vida del proyecto y asegurar que las iniciativas de seguridad [de la información] están en el buen camino para cumplir con los objetivos definidos.*[8]

En este proceso de desarrollo, un CISO/ISM debería tener en cuenta las limitaciones que pueden influir en la estrategia de seguridad de la información:
- Requerimientos legales y regulatorios
- Cultura
- Estructura organizativa
- Costes
- Recursos
- Capacidades
- Tiempo
- Aceptación y tolerancia del riesgo

[8] ISACA, *Manual de Revisión CISM 2012*, EE.UU., 2012, sección 1.9. página 47

La estrategia de seguridad de la información debería abordar, entre otros, los siguientes temas:
- Alineación de las actividades de seguridad de la información con los objetivos generales de la empresa
- Gestión del riesgo de la información–Una descripción de los sistemas de la gestión del riesgo de la información que se implementará en toda la empresa. Este sistema requiere:
  - Una visión empresarial de los objetivos estratégicos y del riesgo
  - Definición de la cantidad de riesgo que la empresa puede asumir a nivel corporativo
  - Una política corporativa sobre las opciones y la selección de la respuesta a los riesgos
  - Supervisión del riesgo
- Un enfoque y principios generales hacia el gobierno y la gestión que describan:
  - Principios y políticas
  - Estructuras organizativas
  - Procesos y prácticas
  - Habilidades, elementos culturales y conductas

Lo anteriormente expuesto es necesario para establecer la dirección y supervisar la seguridad de la información de tal forma que esté alineada con los objetivos de la empresa y el apetito por el riesgo. El gobierno define, entre otros elementos, la responsabilidad de que algo se haga, la responsabilidad de hacer algo y la toma de decisiones.
- Arquitectura de seguridad de la información - Una descripción de los principales conjuntos lógicos de capacidades principales que gestionan la seguridad de la información. Estas capacidades incluyen información, aplicaciones, tecnología y la forma en que todas éstas se relacionan con los procesos de negocio.
- Cumplimiento - Describe todas las reglas y regulaciones que aplican a toda la empresa y el sistema de políticas, procedimientos y todas las demás medidas que la empresa necesita para cumplir con estas regulaciones y para supervisar su cumplimiento de forma continua.
- Operaciones de seguridad de la información - Son los procesos y procedimientos operativos relacionados con la seguridad de la información que incluyen la administración y supervisión de la seguridad de la información, así como la respuesta a los incidentes.
- Hoja de ruta de seguridad de la información - Estado de seguridad deseado incluyendo personas, procesos, tecnología y otros recursos.

E.3 Presupuesto de Seguridad de la Información

Metas
El presupuesto de la seguridad de la información debe ser adecuado (asegurar recursos apropiados), preciso y debe contener cantidades correctas y reales para todos los apartados del presupuesto. Además, el presupuesto debe ser exhaustivo, completo y estar en línea con los requerimientos de seguridad de la organización de la empresa y el apetito general por el riesgo. El presupuesto de la seguridad de la información debe estar disponible a tiempo y ser accesible sólo para aquellos que lo necesitan (p.ej. partes interesadas).

Algunos ejemplos de las métricas para el área de presupuestos incluyen:
- Cantidad de peticiones de presupuesto adicional realizadas tras el presupuesto anual de tal forma que se pueda revisar la evolución del presupuesto
- Cantidad de discrepancias entre el presupuesto de la seguridad de la información y las necesidades en general (p.ej. presupuesto vs estado actual)
- Diferencia entre presupuesto y costes reales
- Porcentaje de partes interesadas sin acceso a l presupuesto de seguridad de la información

Ciclo de Vida
Por lo general las empresas tienen un ciclo presupuestario anual. Los presupuestos de los costes e inversiones relacionados con la seguridad de la información deben seguir este ciclo.

Buena Práctica
Presupuestar en seguridad de la información depende de quién rinde cuentas y de quién es responsable de implementar la seguridad de la información dentro de la empresa. En esta publicación, se asume que la función de la seguridad de la información tiene su propio presupuesto (que es el método más efectivo para asegurar que se proporcionan los recursos de seguridad más apropiados). En tal caso, el CISO/ISM tiene la responsabilidad de desarrollar un presupuesto para la función de seguridad de la información, como parte del presupuesto de la entidad organizativa a la cual reporta la función de seguridad de la información, utilizando el proceso de presupuesto de la organización. Adicionalmente, debe haber una revisión a nivel de toda la empresa de inversiones y gastos relativos a la seguridad de la información.

El propósito del presupuesto de la seguridad de la información es proporcionar financiación al programa de seguridad de la información y posibilitar que el negocio reciba un apoyo apropiado de la seguridad de la información. El programa de seguridad

de la información debe contener todas las inversiones para poder ejecutar la estrategia y arquitectura de la seguridad de la información. En este contexto, es importante disponer de un proceso de asignación de presupuesto adecuado. De acuerdo con el proceso *APO06 Gestionar el presupuesto y costes* de COBIT 5, el presupuesto de la seguridad de la información debe ser desarrollado sobre la base de un Análisis de Impacto en el Negocio (BIA) y los consiguientes requerimientos de negocio, los cuales son traducidos a requerimientos e iniciativas de seguridad de la información. La definición exacta de los requerimientos de la seguridad de la información se discute en la subsección E.6 Requerimientos de Seguridad de la Información.

El presupuesto relacionado con la seguridad de la información puede incluir los siguientes puntos:
- Presupuestos para las operaciones de la función de la seguridad (costes de personal, infraestructura, tecnología, proyectos)
- Presupuesto para el programa de información de seguridad, que puede incluir:
  - Costes e inversiones puntuales para establecer la función de la seguridad de la información y procesos relacionados con la ejecución de proyectos relativos a la seguridad de la información
  - Costes recurrentes en medidas operativas para la seguridad de la información (administración de la seguridad de la información, monitorización, informes, cumplimiento)
  - Costes del programa de concienciación
  - Mejora continua de las habilidades en seguridad de la información (formación de expertos en seguridad, certificaciones, viajes, conferencias)
  - Certificaciones de la seguridad corporativa y costes de la auditoría externa de seguridad
  - Costes del outsourcing
  - Costes de preparación para la respuesta a incidentes

Los presupuestos de seguridad de la información también están sujetos a un seguimiento regular (actual versus presupuestado, variaciones) de acuerdo con las políticas y procesos de la empresa.

E.4 Plan de Seguridad de la Información

Metas

El plan de la seguridad de la información debe ser preciso, exhaustivo y completo, y contener acciones realistas y correctas basadas en la estrategia de la seguridad de la información. Además, debe estar alineado con la arquitectura empresarial y con la situación concreta de la empresa, y en línea con el apetito de riesgo global (p. ej., hay suficiente dinero en el presupuesto). El plan de seguridad debe estar disponible a tiempo y ser accesible sólo para aquellos que lo necesiten (p. ej., partes interesadas).

Estos objetivos pueden ser medidos por métricas incluyendo:
- Número de acciones que no pueden ser implementadas o ejecutadas.
- Número de discrepancias entre el plan de seguridad de la información y la arquitectura empresarial.
- Porcentaje de partes interesadas sin acceso al plan.
- Número de violaciones en contra del plan.

Ciclo de Vida

El plan de la seguridad de la información es creado y después mantenido de manera regular según lo requiera el ISSC, en sincronía con el ciclo presupuestario.

Buena Práctica

El CISO/ISM tiene la responsabilidad de desarrollar un plan de seguridad de la información.

El plan de seguridad de la información se basa en una estrategia de seguridad de la información, que incluye un análisis de riesgos/plan de gestión y responde a todos aquellos riesgos de la información que superen el apetito de riesgo de la empresa. También cubre todos los tipos de respuestas a los riesgos (evitar, mitigar, transferir, aceptar) particularmente la mitigación y la transferencia del riesgo (seguros).

El plan de seguridad de la información define todas las inversiones necesarias para llevar a cabo la estrategia de seguridad de la información y su arquitectura. El plan de seguridad de la información está definido en términos de todos los facilitadores:
- Procesos que necesitan ser definidos, implementados o reforzados
- Estructuras organizativas que necesitan ser creadas o reforzadas
- Flujos de información relacionados con la gestión de la seguridad de la información que necesitan ser implementados
- Políticas y procedimientos que necesitan ser definidos y puestos en práctica
- Cultura de seguridad de la información que necesita ser ajustada o mantenida
- Habilidades y comportamientos que necesitan ser desarrollados o cambiados
- Capacidades que necesitan ser adquiridas, como por ejemplo, tecnología para seguridad de la información, aplicaciones y servicios específicas de seguridad de la información

E.5 Políticas

Las políticas son un tipo importante de información para el gobierno y la gestión de la seguridad de la información. En el marco de trabajo de COBIT 5, las políticas y los principio son también facilitadores del gobierno y la gestión. Por esta razón, puede ser útil referirse al análisis más detallado sobre las políticas en la sección II del capítulo 2 de esta publicación.

E.6 Requerimientos de Seguridad de la Información

Metas

Los requerimientos de la seguridad de información deben ser completos, realistas y alineados con el negocio y con los requisitos legales. Además, los requisitos deben estar disponibles a tiempo y ser accesibles solamente para las partes interesadas (es decir, para aquellos que necesiten acceder).

Ejemplos de métricas para esta área son:
- Número de proyectos con requerimientos de seguridad revisados por la función de seguridad de la información
- Número de requerimientos que no se cumplen
- Número de requerimientos entregados en los proyectos organizativos o que están ausentes en proyectos ya desplegados
- Número de aceptaciones firmadas por los usuarios finales, manifestando recepción y reconocimiento de los requisitos de seguridad más recientes

Ciclo de Vida

Los requerimientos de la seguridad de la información se definen en varios puntos de activación:
- Al comienzo de nuevos proyectos de negocio, como parte del conjunto de los requerimientos de negocio y funcionales—La seguridad de la información es un requerimiento de negocio; los requerimientos de la seguridad de la información son seguidos a lo largo de todo el ciclo de vida de la iniciativa.
- Durante la negociación del contrato/acuerdos con terceras partes.
- Cuando se están investigando adquisiciones/fusiones de compañías (establecer requerimientos para la gestión de las amenazas de las marcas).

Buena Práctica

Los requerimientos de la seguridad de información forman parte del conjunto de los requerimientos de cualquier tipo de catalizador. Esto aplica normalmente a las nuevas capacidades (aplicaciones, infraestructura), aunque también a los restantes catalizadores. Los requerimientos de la seguridad de la información son responsabilidad del usuario final y/o usuario principal, por ejemplo, el propietario del proceso de negocio (para las aplicaciones) o la dirección de TI (para la infraestructura de TI).

Los requerimientos de la seguridad de la información se definen en función del impacto sobre el negocio, objetivos y criterios en términos de:
- **Disponibilidad**—Cuándo ha de estar disponible el catalizador, para quién, en qué medida, etc.
- **Integridad**—Requerimientos de integridad que precisa el catalizador. Aplica a las especificaciones de la información (controles de las aplicaciones sobre transacciones/información), políticas (integridad de las políticas), etc.
- **Confidencialidad**—Quién puede y quién no tener acceso al catalizador. Ejemplos de preguntas frecuentes:
  - En función de las necesidades del puesto de trabajo, ¿quién tiene acceso a la información?
  - ¿Quién tiene acceso a las estructuras organizativas (decisiones) y quién no?

E.7 Material de Concienciación

Metas

Los materiales de concienciación deben ser completos y contener declaraciones realistas y correctas sobre el riesgo y las prácticas. Además, estos materiales deberían ser comprensible y estar adaptados a la mayoría de los puestos de trabajo (considerando el coste). Los empleados necesitan una formación general y orientada al rol desempeñado y sus incentivos deberían estar asociados a la concienciación sobre la seguridad de la información. La formación sobre concienciación en seguridad de la información debería de proporcionarse a todos los empleados y grupos objetivos más importantes y estar accesible solo para aquellos que necesiten acceder (es decir, las partes interesadas).

Las métricas para estas metas pueden incluir:
- Número de actualizaciones en el material de concienciación
- Porcentaje de empleados que han superado determinadas valoraciones en las pruebas
- Porcentaje de empleados que tienen un plan de rendimiento que incluye objetivos de seguridad de la información
- Número de publicaciones aportadas por participantes en respuesta a concursos sobre material de sensibilización

Estás métricas pueden utilizarse para fines administrativos; sin embargo, cabe destacar que la concienciación se puede medir a través del comportamiento y de los efectos de dicho comportamiento, en términos de, por ejemplo, incidencias e incumplimientos.

Ciclo de vida

El material sobre concienciación debe actualizarse periódicamente y/o cuando acontezca un evento determinado (orientado a eventos).

Buena Practica

El material de concienciación puede ayudar a cambiar la forma de pensar y el comportamiento de las personas, lo que mejora globalmente la seguridad de la información. La concienciación fomenta un comportamiento adecuado y el cumplimiento de las políticas, y minimiza los incumplimientos relativos a la seguridad de la información así como comportamientos arriesgados inconscientes.

El material de concienciación deber tomar en consideración todo lo siguiente:

- El diseño y la implementación de un programa efectivo de concienciación en seguridad de la información es apoyado por el compromiso de la dirección ejecutiva.
- El conjunto obligatorio de información está formado por:
  - Las motivaciones de seguridad de la información del negocio
  - La política de la seguridad de la información
  - La política de uso aceptable
  - Los efectos de los incumplimientos, así como un comportamiento peligroso, tanto para la empresa como para el individuo.
- El programa debería aspirar a alcanzar la cultura deseada sobre la seguridad de la información que estará basada en los objetivos empresariales. En compañías que operan internacionalmente, el programa también debería contemplar los aspectos de la cultura local y aceptar ajustes según sea preciso. Sin embargo, se debería establecer una línea base que establezca un nivel mínimo aceptable basada en los valores y los principios comunes de la empresa.
- Las personas representan el grupo objetivo principal. Pueden ser tanto trabajadores internos como trabajadores externos de soporte para la empresa. El material de concienciación se desarrollará para determinados grupos funcionales y grupos según la jerarquía.
- La empresa debería definir e implementar procesos repetitivos de concienciación que servirán para que las partes interesadas cumplan en el día a día con los requerimientos del negocio. Se debería definir el fondo y la forma de dichos procesos.
- La dirección es responsable de prestar soporte al programa de concienciación garantizando la participación de los empleados. RRHH es responsable de los procesos de incorporación y de suministrar el material de concienciación. Los expertos en seguridad de la información son los responsables de proporcionar el contenido en el que se basa el material de concienciación. El CISO/ISM es responsable de que el programa se esté llevando a cabo.
- La tecnología proporciona el medio a través del cual se distribuye el material de concienciación. Por ejemplo, medios de distribución que pueden incluir los canales de comunicación, contenidos activos y formación en línea, encuestas y evaluaciones. El material debe ser ampliamente accesible a través de diversos canales, por ejemplo intranet, documentos y vídeo.
- El material de concienciación se prepara con el apoyo de los expertos de seguridad, RRHH y la dirección de negocio de la empresa. Se puede utilizar en los procesos de incorporación y salida como también en el programa de concienciación. Determinada formación podría ser específica para grupos objetivo.
- Es utilizado como una entrada para el perfil de riesgo, para el diseño de la seguridad de la información y en el programa de gestión de la seguridad de la información.
- El programa de concienciación debe supervisarse y comunicarse a través de:
  - Realización de pruebas que evidencien su comprensión, con fechas en las que se completa y se supera, e informes de las excepciones (no finalización de las pruebas).
  - La supervisión del comportamiento que podría provocar cambios en el material de concienciación: cambios en las amenazas, el negocio, las políticas, los procedimientos y en los incidentes que podrían provocar cambios en el material de concienciación.

Las métricas anteriormente descritas proporcionarán una indicación de la calidad de los productos incluidos en el programa de concienciación desplegado en la empresa. Sin embargo, la eficiencia de las iniciativas de concienciación debe medirse de una forma distinta. Como se ha indicado anteriormente, la medición de la concienciación en la organización requiere de la medida del comportamiento de la compañía, no solamente el cumplimiento con los objetivos administrativos.

E.8 Informes de Revisión de la Seguridad de la Información

Los informes de revisión de la seguridad de información pueden ser de muchos tipos, entre los que se incluyen los siguientes:
- Hallazgos de las auditorias de seguridad de la información
- Informe de madurez de la seguridad de información
- Gestión de riesgos relativos a la seguridad de la información
  - Análisis de amenazas
  - Informe de evaluaciones de vulnerabilidades (seguridad de la información)
  - Análisis de impacto en el negocio (BIA)

En esta sección, el análisis de amenazas se describe en detalle a modo de ejemplo.

Metas
Los informes de revisión de la seguridad de la información deberían ser completos y precisos, con el gasto dirigido a las áreas en las que se han identificado riesgos y con foco en la reducción de los gastos requeridos para recuperarse de las incidencias o vulnerabilidades (incluyendo la minimización de las pérdidas de ingresos). Además, el análisis de amenazas debe identificar todas las amenazas importantes y relevantes para el negocio y debe desarrollar oportunas acciones y respuestas a los riesgos. Los cuadros de mando para las partes interesadas clave deberían actualizarse puntualmente y solamente serán accesibles a quiénes tengan una necesidad de acceso (es decir, las partes interesadas).

Estas metas se pueden medir a través de métricas tales como:
- Número de análisis de amenazas realizados al año
- Número de amenazas identificadas
- Porcentaje de amenazas tratadas en las prácticas de la seguridad de la información
- Porcentaje de actualizaciones ejecutadas según su planificación
- Porcentaje de partes interesadas sin acceso
- Número de violaciones de seguridad de la información

Ciclo de Vida
El análisis de las amenazas se debería actualizar periódicamente y cuando acontezca un evento determinado (orientado a eventos). Los nuevos proyectos o un cambio en las iniciativas de negocio representan ejemplos de eventos que pueden requerir la actualización del análisis de amenazas.

Buena Práctica
Para estar al corriente de las amenazas, el CISO y los gestores de TI y de negocio deberán leer habitualmente artículos de noticias, trabajos de investigación, y tener comunicaciones con los proveedores.

Las pérdidas de datos internas y externas proporcionan información que nos permitan crear los escenarios que se puedan utilizar para el análisis de amenazas.

El análisis de amenazas se tendría que focalizar en las siguientes áreas:
- Debe realizarse un análisis de amenazas a alto nivel para identificar los riesgos de información estratégicos. Por ejemplo, si un banco no cumple con los requerimientos de seguridad de la información dirigidos por la autoridad supervisora local, puede perder su licencia para poder operar.
- Las personas necesitan las habilidades funcionales y el conocimiento apropiados para realizar un análisis de amenazas. Las personas son también una de las fuentes de las violaciones y por tanto contribuyen a la materialización de las amenazas. El factor humano se tendría que considerar siempre que se realiza un análisis de amenazas.
- La función ERM debe definir e implementar el análisis de amenazas como parte del proceso de gestión de riesgos que facilitará a las partes interesadas del negocio la identificación, evaluación, mitigación y prevención de amenazas (de seguridad de información y otras) de una forma preventiva.
- En cierta medida, la tecnología puede ayudar a elaborar el análisis de amenazas mediante la recolección de información. Por ejemplo, la tecnología puede ayudar con el análisis y la correlación de los registros de eventos y mediante el uso de sistemas de gestión de eventos y de información de seguridad (SIEM), utilizando la minería de datos o la inteligencia de negocio para el reconocimiento de patrones, utilizando herramientas de pérdida de información para identificar la fuga de datos y detección del fraude.
- El análisis de amenazas de alto nivel deberían efectuarlo los directores de negocio, por los directores de TI, y por el CISO/ CSO.
- El análisis detallado de las amenazas lo debería realizar expertos de sus áreas respectivas.
- El análisis de las amenazas en un documento confidencial que tiene que ser restringido a los directores principales de negocio, de TI y de seguridad de la información. Debería conservarlo y actualizarlo el CSO/CISO.
- Sirve como entrada para el perfil de riesgo, el diseño de la seguridad de información y el programa de gestión de la seguridad de la información.

E.9 Cuadro de Mando de la Seguridad de la Información

Metas

Los cuadros de mando de la seguridad de información deben contener todos los eventos e información adicional conforme dicten los requerimientos de la seguridad de la información, y la información requerida debe tener un nivel de detalle apropiado para generar acciones. Los cuadros de mando deberían actualizarse puntualmente y solamente ser accesibles para aquellos que necesiten acceder (es decir, las partes interesadas).

Ejemplos de métricas para estas métricas incluyen:
- Número de problemas completos y precisos en el cuadro de mando
- Número de discrepancias entre el cuadro de mando y los requerimientos de seguridad de la información
- Tiempo necesario para analizar el cuadro de mando y obtener la información necesaria
- Porcentaje de actualizaciones ejecutadas según su planificación
- Porcentaje de partes interesadas sin acceso a los cuadros de mando de la seguridad de la información
- Número de violaciones de seguridad de la información del cuadro de mando seguridad de la información

Ciclo de Vida

Los componentes del cuadro de mando deben ser renovados periódicamente. La frecuencia de las actualizaciones dependerá de los tipos de datos y la criticidad. Por ejemplo, la información sobre las incidencias de seguridad puede conllevar como requerimiento actualizaciones en línea inmediatas, mientras que otros componentes, tales como el estado del plan de acción de la seguridad de la información, podrían actualizarse mensualmente.

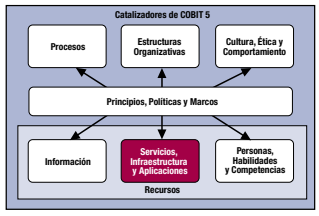
Los informes deben ser almacenados de forma centralizada y ponerlos a disposición de las partes interesadas en un formato de cuadro de mando. Se pueden realizar extractos o resúmenes, en función de las necesidades o del nivel de interés de una parte interesada concreta.

Buena Práctica

El desarrollo y la operación del cuadro de mando tendrá en cuenta lo siguiente:
- El cuadro de mando deberá contener información operativa, así como información sobre las amenazas de seguridad de la información, niveles de amenazas y vulnerabilidades.
- Las personas son el mayor activo de una empresa y parte integral de una implementación satisfactoria de una arquitectura SIEM; no obstante, requieren de las apropiadas habilidades funcionales y de los conocimientos adecuados.
- La empresa debería definir e implementara procesos SIEM repetibles que ayudarán a las partes interesadas del negocio a cumplir en su día a día con los requerimientos del negocio.
- La siguiente información debe formar parte del cuadro de mando y de los informes:
  - La eficiencia y efectividad de las actividades de seguridad de la información
  - Áreas donde es necesaria la mejora
  - Sistemas e información que tienen un nivel de riesgo inaceptable
  - Acciones necesarias para ayudar a minimizar el riesgo en la información (p. ej., revisión del apetito al riesgo de la empresa, comprender el entorno de las amenazas de la seguridad de la información, y apoyar al negocio y a los propietarios de los sistemas a disminuir los riesgos inaceptables)
  - Detalles del progreso realizado desde los informes de supervisión anteriores.
  - Información financiera relativa al coste de los controles de seguridad de la información y el impacto financiero de las incidencias de seguridad de la información.

Página dejada en blanco intencionadamente

Apéndice F
Guía Detallada: Catalizador de Servicios, Infraestructura y Aplicaciones



Este apéndice proporciona detalles relativos a los servicios, la infraestructura y las aplicaciones en el contexto de la seguridad de la información, basándose en el catalizador de servicios, infraestructura y aplicaciones introducido en la sección II. La siguiente lista contiene algunos ejemplos de servicios potenciales relacionados con la seguridad, tal y como podrían figurar en un catálogo de servicios:

- Proporcionar una arquitectura de seguridad.
- Proporcionar concienciación sobre seguridad.
- Proporcionar un desarrollo seguro (desarrollo alineado con los estándares de seguridad).
- Proporcionar evaluaciones de seguridad.
- Proporcionar sistemas adecuadamente asegurados y configurados, en línea con los requerimientos y la arquitectura de seguridad.
- Proporcionar accesos a los usuarios y derechos de acceso de acuerdo con los requerimientos del negocio.
- Proporcionar una adecuada protección frente a software malicioso, ataques externos e intentos de intrusión.
- Proporcionar una adecuada respuesta a incidentes.
- Proporcionar pruebas de seguridad.
- Proporcionar servicios de monitorización y alerta par a eventos relacionados con la seguridad.

Para cada una de estas capacidades de servicio, los bloques de servicios constituyentes se han descrito en este apéndice:

- **Descripción detallada** del servicio, incluyendo funcionalidad de negocio
- **Atributos**—Las entradas y tecnologías de apoyo (incluyendo aplicaciones e infraestructura)
- **Objetivos**—Los objetivos de calidad y cumplimiento para cada capacidad de servicio y las métricas relacionadas

F.1 Arquitectura de Seguridad

Descripción de la Capacidad del Servicio

La **figura 39** describe la capacidad del servicio relativa a la planificación de los servicios.

Figura 39—Planificación de los Servicios: Descripción de la Capacidad del Servicio

Capacidad del Servicio	Descripción
Incluir la seguridad de la información en la arquitectura.	Asegurar la inclusión de requerimientos de la seguridad de la información cuando se analizan discrepancias y se eligen soluciones para la empresa.
Mantener una arquitectura de seguridad.	Mantener un repositorio de arquitectura que contenga estándares de la seguridad de la información, componentes reutilizables, modelos de elementos, relaciones, dependencias y las vistas que permitan la uniformidad en la organización y el mantenimiento de la arquitectura.
Establecer y mantener un inventario de activos.	Proporcionar un inventario detallado de los activos, de la información y físicos, con su adecuada clasificación, propiedad, ubicación, tipo de mantenimiento, valor y criticidad.
Disponer de gestión de la configuración para la seguridad de la información.	La gestión de la configuración proporciona datos que sirven para identificar y hacer progresar los incidentes de la seguridad de la información. Emplear el sistema de gestión de la configuración (CMS) para evaluar el impacto de un incidente e identificar a los usuarios afectados por problemas potenciales. El CMS contiene, además, información relativa a las categorías de los incidentes. Aprovechar el CMS y el mantenimiento de configuraciones estándar, como enfoque proactivo para prevenir incidentes causados por configuraciones desconocidas y para reducir costes.
Establecer y mantener un descubrimiento de la infraestructura.	Poner en marcha el descubrimiento de activos y entidades nuevas que se incorporan o despliegan en un entorno determinado.

Atributos

La **figura 40** describe los atributos de la planificación de los servicios.

Figura 40—Planificación de los Servicios: Atributos		
Capacidad del Servicio	**Tecnología en la que se Apoya**	**Beneficio**
Incluir la seguridad de la información en la arquitectura.	N/A	
Mantener una arquitectura de seguridad.	N/A	
Establecer y mantener un inventario de activos.	• Base de datos de gestión de la configuración (CMDB) • Sistemas de gestión de activos • Protocolo Simple de Gestión de Red (SNMP) • Agentes de provisión de información	• Identificación de los activos en función del tipo de los datos • Protección de los activos de TI deseados • Visión clara del alcance susceptible a ataques externos • Conocimiento claro de los puntos de entrada/salida de la red • Exactitud del inventario • Facilitar la gestión de la configuración • Gestión del análisis coste/beneficio
Disponer de gestión de la configuración para la seguridad de la información.	• CMDB • Escáner de vulnerabilidades • Soluciones de análisis de la actividad en tiempo real en bases de datos • Soluciones de auditoría de políticas	• Facilitar que los estándares de la configuración sean aplicados y supervisados • Identificación de excepciones a los estándares de la configuración • Reducción de las vulnerabilidades
Establecer y mantener un descubrimiento de la infraestructura.	• CMDB • Herramientas de descubrimiento de la red • Sistemas de gestión de activos • SNMP • Agentes de provisión de información	• Identificación de activos nuevos • Protección de los activos de TI deseados • Visión clara del alcance que es susceptible a ataques externos • Conocimiento claro de los puntos de entrada/salida de la red • Exactitud del inventario • Facilitar la gestión de la configuración • Gestión del análisis coste/beneficio

Metas

La **figura 41** describe describe las metas de la planificación de los servicios.

Figura 41—Planificación de los Servicios: Metas		
Capacidad del Servicio	**Objetivo de Calidad**	**Métrica**
Incluir la seguridad de la información en la arquitectura.	Los requerimientos de la seguridad de la información están incluidos en la arquitectura de empresa y se plasman en una arquitectura formal de la seguridad de la información.	Número de excepciones a los estándares de la arquitectura de seguridad.
Mantener una arquitectura de seguridad.	La arquitectura de la seguridad de la información se alinea y evoluciona conforme a los cambios de la arquitectura empresarial.	Fecha de la última revisión y/o actualización de las prácticas de la seguridad de la información aplicadas a la arquitectura empresarial.
Establecer y mantener un inventario de activos.	• Todos los activos se inventarían al completo, de forma precisa, y se mantienen actualizados. • Los activos y entidades nuevos se descubren a su debido tiempo y de forma precisa.	• Número de activos no inventariados • Número de inexactitudes en el inventario • Número de entradas del inventario desactualizados según la fecha. • Coste Total de la Propiedad (TCO) • Número de copias de software ilegal en uso • Reducción de coste/coste no incurrido • Número de activos/entidades sin identificar • Tiempo de demora en descubrir un nuevo activo/entidad

Figura 41—Planificación de los Servicios: Objetivos *(cont.)*		
Capacidad del Servicio	**Objetivo de Calidad**	**Métrica**
Disponer de gestión de la configuración para la seguridad de la información.	Se dispone de una configuración precisa, completa y actualizada de todos los activos y entidades bajo la gestión de la configuración.	• Porcentaje de cambios revocados o revertidos (marcha atrás) • Exactitud de los elementos de configuración y de sus atributos asociados • Eficacia de las pruebas de recuperación • Porcentaje de cambios autorizados frente a los no autorizados • Número de errores en la configuración • Exactitud de las configuraciones gestionadas respecto de aquéllas que se precisan • Número de configuraciones estándar soportadas y frecuencia de los cambios en las configuraciones respecto de los estándares • Número de variaciones identificadas en los elementos de configuración • Tiempo invertido en cambiar los elementos de configuración • Precisión de los cambios en ventanas de cambio concretas y sobre tipos específicos de elementos de configuración. • Número de cambios no planificados sobre elementos de configuración en un periodo de tiempo determinado • Número de cambios revocados o revertidos sobre elementos de configuración. • Número total de elementos de configuración gestionados • Completitud, en relación con el detalle y profundidad, de los atributos de los elementos de configuración
Establecer y mantener un descubrimiento de la infraestructura	Los activos y entidades nuevos pueden descubrirse en tiempo y forma.	• Número de activos/entidades no identificados • Tiempo de demora en descubrir un nuevo activo/entidad

F.2 Concienciación en Seguridad

Descripción de la Capacidad del Servicio

La **figura 42** describe la capacidad del servicio para los servicios de concienciación en seguridad.

Figura 42—Servicios de Concienciación en Seguridad: Descripción de la Capacidad del Servicio	
Capacidad del Servicio	**Descripción**
Proporcionar comunicaciones sobre seguridad de la información posibilitando la concienciación y la formación).	Proporcionar el contenido, el análisis y la entrega de formación, educación, noticias y eventos en seguridad de la información adecuándolos a determinadas entidades o grupos en la empresa.

Atributos

La **figura 43** describe los atributos para los servicios de concienciación en seguridad.

Figura 43—Servicios de Concienciación en Seguridad: Atributos		
Capacidad del Servicio	**Tecnología en la que se Apoya**	**Beneficio**
Proporcionar comunicaciones sobre seguridad de la información posibilitando la concienciación y la formación).	• Cursos de formación (internos y externos) • Canales de noticias • Bases de conocimiento (KBs) • Herramientas de formación • Medios sociales de comunicación • Correo electrónico • Herramientas de colaboración • Avisos de la industria y fabricantes • Avisos CERT	• Incremento de la concienciación en seguridad de la información a lo largo de toda la empresa • Reducción del riesgo mediante ataques de ingeniería social (p.ej., phishing, robo de identidad)

Metas

La **figura 44** describe las metas para los servicios de concienciación en seguridad.

Figura 44—Servicios de Concienciación en Seguridad: Metas		
Capacidad del Servicio	**Objetivo de Calidad**	**Métrica**
Proporcionar comunicaciones sobre seguridad de la información posibilitando la concienciación y la formación).	Formación efectiva y comunicaciones precisas, a tiempo y efectivas sobre seguridad de la información	• Calidad de las comunicaciones que respondan a las necesidades de formación y concienciación sobre seguridad de la información en la empresa. • Grado de completitud respecto a los objetivos definidos sobre concienciación y comunicaciones.

F.3 Desarrollo Seguro

Descripción de la Capacidad del Servicio

La **figura 45** describe la capacidad del servicio para los servicios de desarrollo seguro.

Figura 45—Servicios de Desarrollo Seguro: Descripción de la Capacidad del Servicio	
Capacidad del Servicio	**Descripción**
Desarrollar procedimientos de desarrollo seguro.	El diseño y la entrega de procedimientos de desarrollo, ejemplos y contenido que muestre programación y desarrollo seguro (desarrollo de código resistente ante ataques) para un conjunto de lenguajes y entornos
Desarrollar librerías de infraestructura seguras.	El diseño y la entrega de módulos de seguridad de la información para lenguajes – y entornos – específicos que proporcionen funciones de seguridad de la información críticas o esenciales

Atributos

La **figura 46** describe los atributos para los servicios de desarrollo seguro.

Figura 46—Servicios de Desarrollo Seguro: Atributos		
Capacidad del Servicio	**Tecnología en la que se Apoya**	**Beneficio**
Desarrollar procedimientos de desarrollo seguro.	• Compiladores y enlazadores • Recursos sobre desarrollo seguro (libros, cursos, ejemplos) • Herramientas de análisis binarias y estáticas • Analizadores de código	• Reducción de la posibilidad de vulnerabilidades en el código. • Ayuda a alinearse con los estándares de cumplimiento.
Desarrollar librerías de infraestructura seguras.	• Lenguajes de desarrollo • Recursos sobre desarrollo seguro (libros, cursos) • Analizadores de código • Herramientas de análisis binarias y estáticas • Compiladores y enlazadores	• Protección del capital intelectual • Reducción de la posibilidad de vulnerabilidades en el código.

Metas

La **figura 47** describe las metas para los servicios de desarrollo seguro.

Figura 47—Servicios de Desarrollo Seguro: Metas		
Capacidad del Servicio	**Objetivo de Calidad**	**Métrica**
Desarrollar procedimientos de desarrollo seguro.	Para cada activo o entidad, identificación precisa de toda la información sobre los riesgos, así como de los efectos/ riesgos sobre el negocio.	Número de nuevos tipos de riesgos descubiertos a través de incidentes no contemplados en los informes.
Desarrollo de librerías de infraestructura seguras.	Mejoras en la configuración de la seguridad de la información de los sistemas alineadas con los requerimientos de la seguridad de la información	Número de desviaciones en la seguridad de la información descubiertas tras efectuar una evaluación de la seguridad sobre un sistema bastionado.

F.4 Evaluaciones de Seguridad

Descripción de la Capacidad del Servicio

La **figura 48** describe la capacidad del servicio para los servicios de las evaluaciones de la seguridad.

Figura 48—Servicios de Evaluación de la Seguridad: Descripción de la Capacidad del Servicio	
Capacidad del Servicio	**Descripción**
Efectuar evaluaciones de la seguridad de la información.	Ejecución de una evaluación de la seguridad de la información para una determinada entidad, sistema, proceso, procedimiento, aplicación o unidad organizativa para obtener las desviaciones en la seguridad de la información.
Efectuar evaluaciones de riesgo en la información.	Proceso por el que se proporciona una identificación, evaluación, estimación y análisis de las amenazas y vulnerabilidades para una determinada entidad, sistema, proceso, procedimiento, aplicación o unidad organizativa a fin de determinar los niveles de riesgo asociados (pérdidas potenciales), y hacer uso de dicho análisis como base para identificar las contramedidas rentables más apropiadas así como para determinar el nivel de riesgo aceptable.

Atributos

La **figura 49** describe los atributos para los servicios de evaluación de la seguridad.

Figura 49—Servicios de Evaluación de la Seguridad: Atributos		
Capacidad del Servicio	**Tecnología en la que se Apoya**	**Beneficio**
Realizar evaluaciones de la seguridad de la información.	• Escáner de vulnerabilidades • Fuzzers (herramientas de introducción de datos aleatorios de forma masiva), sniffers (herramienta para escuchar el tráfico de red) • Analizadores de protocolo • Analizadores de red activos y pasivos • Honeypots (sistemas trampa para intrusos) • Agentes de equipos finales • Escáneres de aplicación • Gestión del cumplimiento • Herramientas de informes • Acceso remoto (si se necesitara), redes, canales secundarios, redes privadas virtuales (VPNs)	• Identificación de vulnerabilidades de seguridad de la información • Identificación de agujeros de seguridad que podrían conducir a problemas de cumplimiento
Realizar evaluaciones de los riesgos de la información.	Igual que el anterior: • Escáner de vulnerabilidades • Fuzzers (herramientas de introducción de datos aleatorios de forma masiva), sniffers (herramienta para escuchar el tráfico de red) • Analizadores de protocolo • Analizadores de logs • Analizadores de red activos y pasivos • Honeypots (sistemas trampa para intrusos) • Agentes de equipos finales • Escáneres de aplicación • Gestión del cumplimiento • Herramientas de informes • Acceso remoto (si se necesitara), redes, canales secundarios, redes privadas virtuales (VPNs)	• Provisión de calificación de riesgos para las prácticas de seguridad de la información • Ayuda en la priorización de vulnerabilidades en función del riesgo • Visión de la forma de mitigar riesgos según las necesidades del negocio

Metas

La **figura 50** describe las metas para los servicios de evaluación de la seguridad.

Figura 50—Servicios de Evaluación de la Seguridad: Metas		
Capacidad del Servicio	**Objetivo de Calidad**	**Métrica**
Realizar evaluaciones de la seguridad de la información.	Identificación precisa de todas las debilidades, deficiencias, riesgos, vulnerabilidades y amenazas a un activo o entidad determinada relativas a seguridad de la información	Número de elementos descubiertos a través de incidentes no cubiertos en informes
Realizar evaluaciones de los riesgos de la información.	Identificación precisa de todos los riesgos de la información y riesgos de negocio/efectos resultantes para un activo o entidad determinada	Nuevas áreas de riesgo descubiertas a través de incidentes no cubiertos en los informes

F.5 Sistemas Adecuadamente Asegurados y Configurados, en Línea con los Requerimientos y la Arquitectura de Seguridad

Descripción de la Capacidad de Servicio

La **figura 51** describe la capacidad de servicio para los servicios de sistemas adecuadamente asegurados.

Figura 51—Servicios de Sistemas Adecuadamente Asegurados: Descripción de la Capacidad del Servicio	
Capacidad del Servicio	**Descripción**
Proporcionar sistemas adecuadamente asegurados y configurados, en línea con los requisitos de seguridad de la información y la arquitectura de seguridad.	Proporcionar una configuración, opciones y bastiando de sistemas en seguridad de la información para asegurarse de que la situación de seguridad de la información de un sistema está basada en un conjunto de requisitos o diseños de arquitectura.
Proporcionar seguridad de la información en los dispositivos.	Proporcionar medidas y actividades para la seguridad de la información específicas de dispositivo.
Proporcionar protección al soporte físico de la información.	Proporcionar medidas adecuadas y específicas para la seguridad de la información de datos e información existente en formas no digitales, incluyendo documentos, soportes, instalaciones, perímetro físico y en tránsito.

Atributos

La **figura 52** describe los atributos para los servicios de sistemas adecuadamente asegurados.

Figura 52—Servicios de Sistemas Adecuadamente Asegurados: Atributos

Capacidad del Servicio	Tecnología en la que se apoya	Beneficio
Proporcionar sistemas adecuadamente asegurados y configurados, en línea con los requisitos de seguridad de la información y la arquitectura de seguridad.	• Protocolo de transferencia de archivos (FTP). • Métodos de actualización de la CMDB • Soluciones de verificación de firma • Monitorización de la integridad de ficheros • Módulos del núcleo • Requisitos de seguridad de la información y arquitectura de seguridad de la información • Gestión de sistemas • Gestión de parches • Gestión de la virtualización • Gestión de la nube	• Reducción del acceso no autorizado a los datos • Reducción de las amenazas externas e internas • Simplificación del cumplimiento
Proporcionar seguridad de la información en los dispositivos.	• Plataforma de SO específica para el dispositivo • Consola/sistemas de gestión de la plataforma	• Confidencialidad en caso de robo • Prevención de acceso no autorizado a dispositivos específicos • Información de seguridad más explícita para dispositivos específicos
Proveer protección física a la información.	• Circuito cerrado de televisión • Cerraduras • Alarmas • Control de acceso • Almacenamiento externo • Informes de inteligencia • Interfaces de respuesta inicial • Soluciones de gestión de instalaciones • Sistemas de protección contra incendios • Cerraduras con temporizador • Soluciones de acceso físico	Protección de activos físicos frente a amenazas externas e internas

Metas

La **figura 53** describe las metas para los servicios de sistemas adecuadamente asegurados.

Figura 53—Servicios de Sistemas Adecuadamente Asegurados: Metas

Capacidad del Servicio	Objetivo de Calidad	Métrica
Proporcionar sistemas adecuadamente asegurados y configurados, en línea con los requisitos de seguridad de la información y la arquitectura de seguridad.	Mejoras en la configuración de la seguridad de la información de sistemas de acuerdo con los requerimientos en la seguridad de la información	Número de incidencias de seguridad de la información descubiertas después de una evaluación de la seguridad de la información de un sistema bastionado
Proporcionar seguridad de la información en los dispositivos.	Mejoras en la configuración de la seguridad de la información de los dispositivos de acuerdo con los requisitos de seguridad de la información	Número de incidencias de seguridad de la información descubiertas después de una evaluación de la seguridad de la información de un dispositivo asegurado
Proporcionar seguridad de la información física.	Controles físicos alineados con los requisitos de seguridad de la información	• Número de incidentes no descubiertos en la revisión/evaluación • Número de incidentes detectados no contemplados en los controles existentes

F.6 Acceso de Usuario y Derechos de Acceso de Acuerdo con los Requerimientos del Negocio

Descripción de la Capacidad del Servicio

La **figura 54** describe la capacidad del servicio para los servicios de acceso de usuario y derechos de acceso.

Figura 54—Servicios de Acceso de Usuario y Derechos de Acceso: Descripción de la Capacidad del Servicio

Capacidad del Servicio	Descripción
Proporcionar servicios de autenticación.	Proporcionar un conjunto de capacidades para la realización de la identificación de usuario o entidad utilizando un conjunto de factores según lo determinado por la política de seguridad de la información o los requisitos de control de acceso.
Proporcionar servicios de aprovisionamiento de seguridad de la información.	Proporcionar un conjunto de capacidades para crear, entregar y administrar las tecnologías de seguridad aplicando tecnología a un sistema, entidad, aplicación, servicio o dispositivo determinado.

Figura 54—Servicios de Acceso de Usuario y Derechos de Acceso: Descripción de la Capacidad del Servicio *(cont.)*	
Capacidad del Servicio	**Descripción**
Evaluar los servicios de clasificación de entidades de seguridad de la información.	Evaluar las categorías, clasificación, nivel de seguridad de la información y sensibilidad para una entidad, sistema, proceso, procedimiento, aplicación, servicio o unidad organizativa determinados.
Proporcionar servicios de revocación.	Proporcionar un conjunto de capacidades para la anulación, retirada o terminación de los derechos o capacidades de seguridad de la información para un sistema, entidad, aplicación, servicio, proceso, procedimiento, unidad organizativa o dispositivo determinados.
Proporcionar autenticación de usuario y permisos en línea con los requerimientos del negocio.	Proporcionar un conjunto de capacidades y herramientas de administración para realizar la identificación de usuario mediante un conjunto de factores según lo determinado por la política de seguridad de la información o requisitos de control de acceso tal como se define por los requisitos del negocio.

Atributos

La **figura 55** describe los atributos de los servicios de acceso de usuarios permisos de acceso.

Figura 55—Acceso de Usuarios y Permisos de Acceso a los Servicios: Atributos		
Capacidad del Servicio	**Tecnología en la que se apoya**	**Beneficio**
Proporcionar servicios de autenticación.	• Biométricos • Certificados • Llaves únicas (dongles) • Tarjetas inteligentes Identificación embebida en el dispositivo • Contraseñas de un solo uso (OTPs), llavero con generación de códigos, teléfonos móviles • Usuario/contraseña • Identidad como Servicio (IDaaS), códigos de barras, código universal de producto (UPC) • Lista de revocación de certificados (CRL), federación de identidades • Certificados raíz • Servicios de gestión de claves • Servicios de localización • Servicios de reputación • Infraestructura de clave pública (PKI)	• Prevención de acceso no autorizado a sistemas/datos • Aseguramiento de que cada entidad dispone únicamente del nivel de acceso necesario • La salvaguarda de información confidencial • Verificación de la identidad de los usuarios que acceden a los sistemas
Proporcionar servicios de aprovisionamiento de seguridad de la información.	• Aprovisionamiento Open Mobile Alliance (OMA) Device Management (DM) • Módulo de identidad del abonado (SIM), certificados, certificados raíz • Servicios de cifrado local y remoto • Servicios de gestión de claves • Servicios de distribución de software • Recepción de datos desde RRHH	Acceso apropiado y en tiempo para los empleados a los sistemas necesarios
Proporcionar seguridad de la información a los servicios de clasificación de entidades.	• Diagramas y herramientas de visualización • Herramientas de clasificación • CMDB • Arquitectura empresarial • Normas de clasificación • Soluciones de traspaso a producción de versiones candidatas (*release candidate*)	Habilita agrupaciones y categorizaciones apropiadas de las entidades de seguridad de la información para clasificar el nivel de riesgo apropiado
Proporcionar servicios de revocación.	• SIM, certificados y certificados raíz • Servicios de cifrado local y remoto • Servicios de gestión de claves • Servicios de localización • Recepción de datos desde RRHH • PKI	• Prevención del acceso a los sistemas por parte de usuarios no autorizados después de que se hayan revocado sus privilegios (debido a la finalización de contrato o cambio de rol) • Reducción de la probabilidad de un ataque interno
Proporcionar autentificación de usuario y derechos de autorización de acuerdo con los requisitos del negocio.	• SIM, certificados y certificados raíz • Servicios de cifrado local y remoto • Servicios de gestión de claves • Servicios de localización • PKI	• Verificación de que los usuarios tienen el nivel apropiado de acceso sólo a los sistemas necesarios • Reducción de la exposición de datos sensibles • Reducción de la probabilidad de ataque interno

Metas

La **figura 56** describe describe las metas para los servicios de acceso de usuario y permisos de acceso.

Figura 56—Servicios de Sistemas Adecuadamente Asegurados: Metas		
Capacidad del Servicio	**Objetivo de Calidad**	**Métrica**
Proporcionar servicios de autenticación.	Autenticación precisa, completa y en tiempo de todas las entidades y/o servicios	• Número de entidades o servicios que no se encuentran bajo el servicio de autentificación • Integridad de los factores de autenticación apoyando los requisitos de seguridad de la información
Proporcionar servicios de aprovisionamiento de seguridad de la información.	Aprovisionamiento preciso, completo y en tiempo de todos los servicios y elementos de seguridad de la información para entidades, dispositivos o servicios	• Número de transacciones de aprovisionamiento incompletas • Número de transacciones de aprovisionamiento imprecisas • Retardo medio del aprovisionamiento • Violación del máximo retardo en aprovisionamiento
Evaluar los servicios de clasificación de entidades de seguridad de la información.	Clasificación de todas las identidades precisa y completa	• Número de imprecisiones en la clasificación • Número de clases no definidas para entidades descubiertas • Número de cambios requeridos para clasificaciones existentes
Proporcionar servicios de revocación.	Revocación de todas las identidades y/o servicios de forma precisa, completa y en tiempo	• Número de revocaciones fallidas para objetivos • Integridad de revocaciones soportando los requisitos de seguridad de la información • Retraso en la revocación de entidades y servicios para un objetivo determinado
Proporcionar autenticación de usuario y permisos en línea con los requerimientos del negocio.	Autenticación precisa, completa y en tiempo junto con la autorización apropiada para todas las entidades y/o servicios	• Número de entidades o servicios que no se encuentran bajo el servicio de autenticación o autorización • Integridad de los factores de autenticación y autorización apoyando los requisitos de seguridad de la información y de negocio

F.7 Protección Adecuada Frente a Software Malicioso (*Malware*), Ataques Externos e Intentos de Intrusión

Descripción de la Capacidad de Servicio

La **figura 57** describe la capacidad de servicio para la protección frente a software malicioso (*malware*) y ataques.

Figura 57—Protección Frente a Software Malicioso (Malware) y Ataques: Descripción de la Capacidad de Servicio	
Capacidad de Servicio	**Descripción**
Proporcionar seguridad de la información y las contramedidas para amenazas (internas o externas).	Planificar, implementar, mantener y mejorar las medidas, contramedidas y actividades, incluyendo, pero no limitado a acciones, procesos, dispositivos o sistemas, frente a las amenazas y las vulnerabilidades identificadas en las evaluaciones de riesgos, políticas de seguridad de la información y la estrategia de seguridad de la información. Estar al tanto de tecnologías emergentes.
Proporcionar protección de datos (en servidor, red, nube y almacenamiento).	Proporcionar un conjunto de capacidades y prácticas de gestión para implementar la protección, la confidencialidad, integridad y disponibilidad de los datos en todos los estados incluyendo, pero no limitado a, en reposo o en tránsito, local y exteriormente, a corto y a largo plazo.

Atributos

La **figura 58** describe los atributos para la protección frente a software malicioso (*malware*) y ataques.

Figura 58—Protección Frente a Software Malicioso (*Malware*) y Ataques: Atributos		
Capacidad del Servicio	**Tecnología en la que se Apoya**	**Beneficio**
Proporcionar seguridad de la información y las contramedidas para amenazas (internas o externas).	• Cifrado • PKI, inspección profunda de paquetes (DPI), sniffers (herramienta para escuchar el tráfico de red) • Cortafuegos • Analizador de paquetes, sensores • Gestión del cumplimiento • Requisitos y arquitectura de seguridad de la información • CMDB • Gestión del sistema de parches • Gestión de la virtualización • Gestión de la nube • Cuadros de mando proporcionados por el proveedor y agentes de gestión • Actualizaciones proporcionadas por el proveedor • Repositorios de software abierto (OSS) • Avisos de seguridad de la información del proveedor, bases de conocimiento, honeypots (sistemas trampa), tarpits (envíos diferidos de correos y a bajos ratios de intensidad) • Anti-software malicioso, anti-rootkits, anti-software espía, anti-phishing • Protección del navegador, sandboxing (entornos aislados), inspección del contenido • Servicios de reputación	• Referencias actualizadas para remediar las amenazas • Prevención de ataques internos y externos
Proporcionar protección de datos (en servidor, red, nube y almacenamiento).	• PKI, sniffers, DPI • Servicios de cifrado • Prevención de pérdida de datos (DLP) • Soluciones de gestión de sistemas y dispositivos • Soluciones de distribución de software • Sistemas de administración remota • Soluciones de gestión de virtualización y nube • Gestión documental • Sistemas de clasificación de datos • Soluciones de gestión de datos centrados en la aplicación • Soluciones de ofuscación de datos	• Capacidad para que los datos sean almacenados y transferidos con seguridad • Confidencialidad, integridad y disponibilidad

Metas

La **figura 59** describe los objetivos para la protección frente a software malicioso (*malware*) y ataques.

Figura 59—Protección Frente a Software Malicioso (*Malware*) y Ataques: Metas		
Capacidad de Servicio	**Objetivo de Calidad**	**Métrica**
Proporcionar seguridad de la información y las contramedidas para amenazas (internas o externas).	Máxima protección contra amenazas conocidas y desconocidas	Número de incidentes relacionados con la seguridad de la información
Proporcionar protección de datos (en servidor, red, nube y almacenamiento).	Máxima protección de datos en todos los estados	Número de exposiciones de los datos

F.8 Respuesta a Incidentes Adecuada

Descripción de la Capacidad de Servicio

La **figura 60** describe la capacidad de servicio para los servicios de respuesta a incidentes.

Figura 60—Servicios de Respuesta a Incidentes: Descripción de la Capacidad de Servicio	
Capacidad de Servicio	**Descripción**
Proveer un servicio de escalado en la seguridad de la información.	Proveer un conjunto de capacidades y prácticas de gestión (incluyendo, pero no limitado a, escalados funcionales y jerárquicos) para resolver los incidentes relacionados con seguridad de la información a tiempo
Proporcionar (análisis) forenses para seguridad de la información.	Proporcionar un conjunto de capacidades que permiten a los forenses actuar en una entidad, sistema, proceso, procedimiento, aplicación, servicio, dispositivo o unidad organizativa (o agrupación de los mismos) dados para apoyar en las investigaciones, descubrimiento electrónico y recogida de pruebas. Asegurar que se realiza el conjunto de capacidades para permitir un tratamiento legal y el mantenimiento de la cadena de custodia tal y como es requerido por los procedimientos legales / gubernamentales

Atributos
La **figura 61** describe los atributos para los servicios de respuesta a incidentes.

Figura 61—Servicios de Respuesta a Incidentes: Atributos		
Capacidad de Servicio	**Tecnología en la que se Apoya**	**Beneficio**
Proveer un servicio de escalado en la seguridad de la información.	• Gestión de vulnerabilidades • Recomendaciones de seguridad de la información de los proveedores • Recomendaciones de seguridad de la industria de la información • Sistema de escalado jerárquico (basado en la organización) • Políticas de seguridad de la información	Resolución en tiempo, de incidentes relacionados con la seguridad de la información estableciendo un camino jerárquico para el escalado
Proporcionar (análisis) forenses para seguridad de la información.	• Herramientas de inspección de memoria • Analizadores de red • Analizadores de registros • Herramientas de inspección de aplicaciones y datos • Herramientas de ingeniería inversa • Herramientas de análisis de código malicioso (*malware*) • Conjunto de herramientas forenses de fabricante y fuentes de código abierto (OSS) • Tráfico de red • Módulos de software malicioso y código • SIEM	Soporte para la investigación y descubrimiento de información relacionada con incidentes de seguridad

Metas
La **figura 62** describe las metas para los servicios de respuesta a incidentes.

Figura 62—Servicios de Respuesta a Incidentes: Metas		
Capacidad de Servicio	**Objetivo de Calidad**	**Métrica**
Proveer un servicio de escalado en la seguridad de la información.	Procedimientos de escalado en tiempo, precisos, efectivos, eficientes y orientados	• Número de escalados imprecisos, no efectivos, ineficientes o mal dirigidos • Retraso en las comunicaciones de escalado
Proporcionar (análisis) forenses para seguridad de la información.	Análisis y recopilación de información precisa, completa y descubrible	Resultados de análisis forense imprecisos, incompletos o inadmisibles

F.9 Pruebas de Seguridad

Descripción de la Capacidad de Servicio
La **figura 63** describe la capacidad de servicio para los servicios de pruebas de seguridad.

Figura 63—Servicios de Pruebas de Seguridad: Descripción de la Capacidad de Servicio	
Capacidad de Servicio	**Descripción**
Realizar pruebas de la seguridad de la información.	Proporcionar servicios de prueba y evaluación de la seguridad de la información, incluyendo, pero no limitado a, realizar pruebas para la protección de datos y validación de la integridad, análisis de regresión basado en la seguridad de la información, pruebas de seguridad y marcos de trabajo, y aseguramiento de la calidad, con el objetivo final de mantener la funcionalidad de la seguridad de la información tal y como se pretende.

Atributos
La **figura 64** describe los atributos para los servicios de pruebas de seguridad.

Figura 64— Servicios de Pruebas de Seguridad: Atributos		
Capacidad de Servicio	**Tecnología en la que se Apoya**	**Beneficio**
Realizar pruebas de la seguridad de la información	• Herramientas de seguridad de la información • Herramientas de desarrollo de software (SDKs) • Métodos de arranque alternativo • Herramientas de análisis de regresión • Herramientas de prueba de seguridad de la información • Herramienta de pruebas unitarias y sistemas	• Aumento de la concienciación en seguridad de la información • Conocimiento general de las vulnerabilidades sobre la seguridad de la información dentro de la empresa • Oportunidad para reducir vulnerabilidades en etapas tempranas

Metas

La **figura 65** describe las metas para los servicios de pruebas de seguridad.

Figura 65—Servicios de Pruebas de Seguridad: Objetivos		
Capacidad de Servicio	**Objetivo de Calidad**	**Métrica**
Realizar pruebas sobre la seguridad de la información.	Mejoras en la configuración de la seguridad de la información del dispositivo de acuerdo con los requerimientos de seguridad de la información.	Número de incidencias de seguridad de la información descubiertas después de una evaluación de la seguridad de la información del dispositivo asegurado.

F.10 Servicios de Monitorización y Alerta para Eventos relacionados con la Seguridad

Descripción de la Capacidad de Servicio

La **figura 66** describe la capacidad de servicio para los servicios de monitorización y mejora de la seguridad de la información.

Figura 66—Servicios de Monitorización y Mejora de la Seguridad de la Información: Descripción de la Capacidad de Servicio	
Capacidad de Servicio	**Descripción**
Proporcionar servicios de monitorización de los procesos y eventos de seguridad de la información.	Proporciona un conjunto de capacidades que permiten, tanto en tiempo real como en diferido, la monitorización y los cuadros de mando que apoyan los datos necesarios y la correlación de eventos y su integración.
Proporcionar servicio de alerta y notificación de las prácticas, procesos y eventos de seguridad de la información.	Proporciona un conjunto de capacidades para permitir, tanto en tiempo real y post evento, alertar, informar y correlacionar eventos, incidentes, procesos y acciones etiquetadas, así como el apoyo para el escalado y remediación adecuados.
Proporcionar mediciones y métricas de seguridad de la información (indicadores clave de objetivo (KGIs), indicadores clave de rendimiento (KPIs), etc.).	Proporciona un conjunto de capacidades que envían medidas, métricas y análisis de seguridad de la información en los que se miden las prácticas y objetivos de seguridad de la información en contraste con los criterios de rendimiento actual y deseado.

Atributos

La **figura 67** describe los atributos para los servicios de monitorización y mejora de la seguridad de la información.

Figura 67—Monitorizar y Mejorar los Servicios de la Seguridad de la Información: Atributos		
Capacidad de Servicio	**Tecnología en la que se Apoya**	**Beneficio**
Proporcionar servicios de monitorización de los procesos y eventos de seguridad de la información.	• Logs • SNMP • Sistema de Alertas • SIEM • Gestión de cuadros de mando • Centro de operaciones de red (NOCs)	Monitorización en tiempo real de eventos apropiados
Proporcionar servicio de alerta y notificación de las prácticas, procesos y eventos de seguridad de la información.	• Logs • SNMP • Sistema de Alertas • SIEM • Gestión de cuadros de mando • Centro de operaciones de red (NOCs)	Respuesta apropiada para eventos de seguridad de la información
Proporcionar mediciones y métricas de seguridad de la información (KGIs, KPIs, etc.).	• Hojas de cálculo y métricas estándar • SIEM • Gestión de cuadros de mando • Cuadros de mando • Sistemas de alerta • Herramientas de respuesta a incidentes • Políticas de seguridad de la información	• Medida del rendimiento • Datos cuantificables

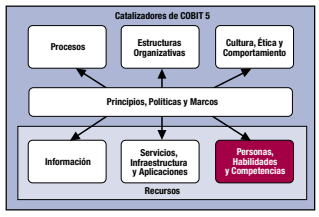
Metas

La **figura 68** describe las metas para los servicios de monitorización y mejora de la seguridad de la información.

Figura 68—Servicios de Monitorización y Mejora de la Seguridad de la Información: Metas

Capacidad de Servicio	Objetivo de Calidad	Métrica
Proporcionar servicios de monitorización de los procesos y eventos de seguridad de la información.	Monitorización precisa y completa de todos los procesos y eventos relevantes de seguridad de la información	Número de eventos monitorizados/registrados imprecisos o incompletos
Proporcionar servicio de alerta y notificación de las prácticas, procesos y eventos de seguridad de la información.	Alerta precisa, completa y en tiempo de todos los eventos relevantes o críticos de seguridad de la información	• Número de alertas de eventos imprecisas o incompletas • Retraso en la alerta de eventos críticos de seguridad de la información
Proporcionar mediciones y métricas de seguridad de la información (KGIs, KPIs, etc.).	Medidas precisas y completas de seguridad de la información que se alineen con la estrategia de seguridad de la información	• Calidad e integridad de los indicadores clave de objetivo (KGIs) y los indicadores clave de rendimiento (KPIs) • Número de errores de medición

Apéndice G
Guía Detallada: Catalizador de Personas, Habilidades y Competencias



Este apéndice contiene información detallada sobre un conjunto de habilidades y competencias, basada en la introducción del catalizador personas, habilidades y competencias de la sección II:
- El gobierno de la seguridad de la información
- La formulación de la estrategia de seguridad de la información
- La gestión de riesgos de la información
- El desarrollo de la arquitectura de seguridad de la información
- Las operaciones de seguridad de la información
- La evaluación, las pruebas y el cumplimiento de la información

Para cada una de estas habilidades y competencias, se describen los siguientes atributos:
- La descripción y definición de las habilidades
- La experiencia, formación y cualificaciones requeridas para la habilidad/competencia
- El conocimiento, las habilidades técnicas y las habilidades en el comportamiento
- La estructura relacionada (si aplica)

G.1 Gobierno de la Seguridad de la Información

Descripción y Definición de la habilidad
Esta habilidad establece y mantiene un marco para la seguridad de la información y los procesos que lo soportan para asegurar que la estrategia de la seguridad de la información está alineada con las metas y objetivos de la organización, los riesgos de la información son gestionados adecuadamente y los recursos del programa son gestionados de manera responsable.

Experiencia, Formación y Cualificaciones Requeridas para la Habilidad/Competencia
La **figura 69** describe la experiencia y cualificaciones para el gobierno de la seguridad de la información.

Figura 69—Gobierno de la Seguridad de la Información: Experiencia, Educación y Cualificaciones

Requerimiento	Descripción
Experiencia	Varios años de experiencia en seguridad de la información y gestión de TI/negocio (recomendado) incluyendo experiencia en: • Creación, implementación y medida de políticas de seguridad de la información • Cumplimiento de seguridad de la información con regulaciones externas • Alineamiento de la estrategia de la seguridad de la información con el gobierno corporativo • Creación de políticas de la seguridad de la información alineadas con las necesidades del negocio e ideando métodos para medir la efectividad de las políticas • Comunicación con la dirección ejecutiva
Cualificaciones	CISM

Conocimiento, Habilidades Técnicas y Habilidades en el Comportamiento
La **figura 70** describe el conocimiento, las habilidades técnicas y las habilidades en el comportamiento para el gobierno de la seguridad de la información.

Figura 70—Gobierno de la Seguridad de la Información: Conocimiento, Habilidades Técnicas y Habilidades en el Comportamiento

Requerimiento	Descripción
Conocimiento	Habilidad para: • Definir métricas que apliquen al gobierno de la seguridad de la información • Crear un modelo de medición del rendimiento basado en las métricas de gobierno de seguridad de la información que asegure que se alcanzan los objetivos de la organización • Desarrollar un caso de negocio que justifique las inversiones en seguridad de la información Conocimiento de: • Requisitos legales y regulatorios que afecten a la seguridad de la información • Roles y responsabilidades necesarios para la seguridad de la información en la empresa • Métodos para implementar las políticas de gobierno de la seguridad de la información • Conceptos fundamentales de gobierno y como se relacionan con la seguridad de la información • Normas reconocidas internacionalmente, marcos y buenas prácticas relacionadas con el gobierno de la seguridad de la información y el desarrollo de la estrategia

Figura 70—Gobierno de la Seguridad de la Información: Conocimiento, Habilidades Técnicas y Habilidades en el Comportamiento *(cont.)*	
Requerimiento	**Descripción**
Habilidades técnicas	Buen conocimiento de las prácticas de seguridad de la información que se aplican al negocio específico
Habilidades en el comportamiento	• Líder contrastado con excelentes habilidades de comunicación • Orientación a los procesos

G.2 Formulación de la Estrategia de Seguridad de la Información

Descripción y Definición de la habilidad

Esta habilidad define e implementa la visión, misión y objetivos de la seguridad de la información alineados con la estrategia y cultura corporativa.

Experiencia, Formación y Cualificaciones Requeridas para la Habilidad/Competencia

La **figura 71** describe la experiencia, formación y cualificaciones para la formulación de la estrategia de seguridad de la información.

Figura 71—Formulación de la Estrategia de Seguridad de la Información: Experiencia, Formación y Cualificaciones	
Requerimiento	**Descripción**
Experiencia	Varios años de experiencia en seguridad de la información y gestión de TI/negocio (recomendado) incluyendo: • Experiencia en estrategia y gobierno de la seguridad de la información • Experiencia en creación e implementación de estrategias y principios, prácticas y actividades de seguridad de la información • Un amplio conocimiento de las funciones de la seguridad de la información y como se relacionan con el negocio
Cualificaciones	CISM

Conocimiento, Habilidades Técnicas y Habilidades en el Comportamiento

La **figura 72** describe el conocimiento, las habilidades técnicas y las habilidades en el comportamiento para la formulación de la estrategia de seguridad de la información.

Figura 72—Formulación de la Estrategia de Seguridad de la Información: Conocimiento, Habilidades Técnicas y Habilidades en el Comportamiento	
Requerimiento	**Descripción**
Conocimiento	Habilidad para: • Entender la cultura y los valores de la empresa • Definir una estrategia de seguridad de la información que esté alineada con la estrategia de la empresa • Desarrollar políticas de seguridad de la información e idear métricas que midan la efectividad de las políticas Conocimiento de: • Tendencias, servicios y disciplinas de seguridad de la información • Requisitos legales y regulatorios que afecten a la seguridad de la información • Estándares reconocidos internacionalmente, marcos y buenas prácticas relacionados con el desarrollo de una estrategia de seguridad de la información
Habilidades técnicas	Amplio conocimiento de gestión de las identidades de acceso, gestión de las amenazas y vulnerabilidades, arquitectura de seguridad de la información y protección de datos
Behavioural skills	• Líder contrastado con excelentes habilidades de comunicación y la capacidad para interactuar con todos los niveles de la empresa • Orientación a negocio • Pensamiento estratégico de alto nivel • Entendimiento del entorno

Roles/Estructuras relacionados

La **figura 73** describe los roles/estructuras para la formulación de la estrategia de seguridad de la información.

Figura 73—Formulación de la Estrategia de Seguridad de la Información: Roles/ Estructuras relacionados
Roles/Estructuras relacionados
CISO
ISSC

G.3 Gestión de Riesgos de Seguridad de la Información

Definición y Descripción de la habilidad

Esta habilidad asegura que los riesgos de información se gestionan para cumplir con las directivas de ERM.

Experiencia, Formación y Cualificaciones Requeridas para la Habilidad/Competencia

La **figura 74** describe la experiencia, formación y cualificaciones para la gestión de los riesgos de información.

Figura 74—Gestión de Riesgos de Información: Experiencia, Formación y Cualificaciones

Requerimiento	Descripción
Experiencia	Varios años de experiencia en seguridad de la información y gestión de negocio/TI (recomendado) incluyendo experiencia en: • Evaluar el riesgo relativo a las prácticas de seguridad de la información • Mitigar el riesgo basado en las necesidades de negocio de la empresa • Gestión del riesgo, perfiles de riesgo y evaluación de amenazas
Cualificaciones	CRISC

Conocimiento, Habilidades Técnicas y Habilidades de Comportamiento

La **figura 75** describe el conocimiento, las habilidades técnicas y las habilidades de comportamiento para la gestión de los riesgos de información.

Figura 75—Gestión de Riesgos de Información: Conocimiento, Habilidades Técnicas y Habilidades de Comportamiento

Requerimiento	Descripción
Conocimiento	Conocimiento de: • Métodos para establecer un modelo de clasificación de activos de información consistente con los objetivos de negocio • Metodologías de análisis y evaluación de riesgos • Procesos y funciones esenciales de negocio • Estándares de la industria de seguridad de la información (p.ej., NIST, PCI) • Leyes y regulaciones relacionadas con la seguridad de la información (p.ej. legislación de privacidad local y regional) • Marcos y modelos de riesgos, cuantificación de riesgos, registro de riesgos e informes de riesgos
Habilidades técnicas	• Comprensión de las prácticas y actividades de seguridad de la información y del riesgo asociado a ellas • Análisis de riesgos y controles de mitigación
Habilidades de comportamiento	• Pensamiento abstracto • Experiencia en resolver problemas • Orientación a procesos

G.4 Desarrollo de la Arquitectura de Seguridad de la Información

Definición y Descripción de la habilidad

Esta habilidad supervisa el diseño e implementación de la arquitectura de seguridad de la información.

Experiencia, Formación y Cualificaciones Requeridas para la Habilidad/Competencia

La **figura 76** describe la experiencia, formación y cualificaciones para el desarrollo de la arquitectura de seguridad de la información.

Figura 76—Desarrollo de la Arquitectura de Seguridad de la Información: Experiencia, Formación y Cualificaciones

Requerimiento	Descripción
Experiencia	Varios años de experiencia en seguridad de la información (recomendado) incluyendo: • Experiencia trabajando con sistemas hardware y software, incluyendo sistemas operativos, bases de datos, aplicaciones y redes • Comprensión técnica de cómo varios sistemas se interconectan unos con otros
Cualificaciones	• Buen entendimiento de protocolos de red, bases de datos, aplicaciones y sistemas operativos y cómo son aplicables a los procesos de negocio • CRISC, CISSP

Conocimiento, Habilidades Técnicas y Habilidades de Comportamiento

La **figura 77** describe el conocimiento, las habilidades técnicas y las habilidades de comportamiento para el desarrollo de la arquitectura de seguridad de la información.

Figura 77—Desarrollo de la Arquitectura de Seguridad de la Información: Conocimiento, Habilidades Técnicas y Habilidades de Comportamiento

Requerimiento	Descripción
Conocimiento	Conocimiento de: • Como todas las tecnologías de la empresa interactúan con el negocio y con las políticas de seguridad de la información • Arquitecturas de seguridad de la información (p. ej. Sherwood Applied Business Security Architecture [SABSA], The Open Group Architecture Framework [TOGAF] y procedimientos que les aplican • Revisión del diseño de aplicación y modelado de amenazas • Métodos para diseñar prácticas de seguridad de la información • Gestión de programas informáticos, políticas, procedimientos y estándares de seguridad de la información en relación a las actividades del negocio • Estándares/buenas prácticas de la industria de seguridad de la información (p. ej. serie ISO/IEC 27000, ISF, NIST, PCI) • Leyes y regulaciones referentes a seguridad de la información • Tecnologías emergentes de seguridad de la información y desarrollo de metodologías
Habilidades técnicas	• Conocimiento profundo y global de TI y tendencias emergentes • Capacidades de diseño técnico • Amplia experiencia en operación de equipos informáticos
Habilidades de comportamiento	• Pensamiento abstracto • Experiencia en resolver problemas

Rol/Estructura Relacionada

La **figura 78** describe el rol/estructura relacionada para el desarrollo de la arquitectura de seguridad de la información.

Figura 78—Desarrollo de la Arquitectura de Seguridad de la Información: Rol/Estructura relacionada

Rol/Estructura relacionada
ISM
Arquitecto de seguridad de la información

G.5 Operaciones de Seguridad de la Información

Definición y Descripción de Habilidades

Esta habilidad gestiona el programa de seguridad de la información en línea con la estrategia de seguridad de la información. Incluye:

- Planificar, establecer y gestionar la capacidad de detectar, investigar, responder y recuperarse de incidentes de seguridad de la información para minimizar el impacto en el negocio
- Realizar las tareas de aprovisionamiento de usuarios para los sistemas empresariales y entornos de aplicaciones
- Apoyar en la definición de roles y modelos de acceso para las plataformas y entornos y aplicaciones
- Supervisar y mantener las plataformas tecnológicas y soluciones de gestión de accesos que soportan las capacidades de gestión de accesos
- Gestionar la seguridad de la información en redes y conectividades
- Gestionar la seguridad de la información de los equipos finales
- Proteger frente al software malicioso
- Tratar los incidentes de seguridad y gestión de eventos

Experiencia, Formación y Cualificaciones Requeridas para la Habilidad/Competencia

La **figura 79** describe la experiencia, formación y cualificaciones para las operaciones de seguridad de la información.

Figura 79—Operaciones de Seguridad de la Información: Experiencia, formación y cualificaciones

Requerimiento	Descripción
Experiencia	Experiencia en seguridad de la información/TI (recomendado) incluyendo: • Conocimientos muy consolidados de seguridad de la información • Conocimientos sólidos de todas las funciones de seguridad de la información de una empresa y comprensión de cómo se alinean con los objetivos de negocio
Cualificaciones	• Experiencia en implementar directivas del programa de seguridad de la información para proteger los activos de la empresa, minimizando el riesgo corporativo, las obligaciones y las pérdidas • CRISC, CISSP • Certificaciones específicas de proveedores y de tecnologías

Conocimiento, Habilidades Técnicas y Habilidades de Comportamiento

La **figura 80** describe el conocimiento, las habilidades técnicas y las habilidades de comportamiento para las operaciones de seguridad de la información.

Figura 80—Operaciones de Seguridad de la Información: Conocimiento, Habilidades Técnicas y Habilidades de Comportamiento	
Requerimiento	**Descripción**
Conocimiento	Conocimiento de: • Gestión de programas informáticos, políticas, procedimientos y estándares de seguridad de la información en relación a las actividades del negocio • Monitorización, consolidación y análisis de de registros de log
Habilidades técnicas	• Amplia experiencia en operaciones informáticas • Conocimientos sólidos de sistemas operativos Windows/UNIX, métodos de autenticación, cortafuegos, enrutadores (router), servicios web, etc.
Habilidades de comportamiento	• Habilidad para la gestión de proyectos y personal • Mentalidad analítica y detallada • Sólidas habilidades de comunicación y mediación • Sólidas técnicas de gestión del tiempo

Rol/Estructura relacionada

La **figura 81** describe el rol/estructura relacionada para las operaciones de seguridad de la información.

Figura 81— Operaciones de Seguridad de la Información: Rol/Estructura relacionada
Rol/Estructura relacionada
ISM
Administrador de seguridad de la información

G.6 Evaluación, Pruebas y Cumplimiento de la Información

Definición y Descripción de la habilidad

Esta habilidad asegura que el procesamiento y manejo de la información sea conforme a las leyes, regulaciones, directivas y estándares internas y externas.

Experiencia, Formación y Cualificaciones Requeridas para la Habilidad/Competencia

La **figura 82** describe la experiencia, formación y cualificaciones para la evaluación, pruebas y cumplimiento de la información.

Figura 82—Evaluación, Pruebas y Cumplimiento de la Información: Experiencia, Formación y Cualificaciones	
Requerimiento	**Descripción**
Experiencia	Varios años de experiencia en seguridad de la información y auditoría/cumplimiento (recomendado) incluyendo experiencia en: • Auditar, conforme a las leyes y regulaciones que la empresa debe de cumplir • Asegurar que las prácticas documentadas de seguridad de la información son efectivas y se están cumpliendo
Cualificaciones	Certificación en auditoría de seguridad de la información y actividades de cumplimiento (CISA)

Conocimiento, Habilidades Técnicas y Habilidades de Comportamiento

La **figura 83** describe el conocimiento, las habilidades técnicas y las habilidades de comportamiento para la evaluación, pruebas y cumplimiento de la información.

Figura 83—Evaluación, Pruebas y Cumplimiento de la Información: Conocimiento, Habilidades Técnicas y Habilidades de Comportamiento	
Requerimiento	**Descripción**
Conocimiento	Conocimiento de: • Estándares de auditorías, guías y buenas prácticas de seguridad de la información que aseguren que los sistemas de negocio están protegidos y gestionados • Técnicas de gestión de proyectos de auditoría y planificación de auditorías • Estándares de la industria de seguridad de la información (p.ej.,series ISO/IEC 27000, ISF, NIST, PCI) • Leyes y legislaciones locales referentes a seguridad de la información (p.ej., US Gramm-Leach-Billey Act [GLBA]
Habilidades técnicas	Herramientas propias de auditoría, amplio conocimiento TI, análisis de discrepancias
Habilidades de comportamiento	• Altos valores éticos • Orientación a procesos • Excelentes capacidades de negociación

Página dejada en blanco intencionadamente

Apéndice H
Mapeos Detallados

Este apéndice proporciona un mapeo a alto nivel entre varios estándares y marcos de referencia en el área de seguridad de la información y *COBIT 5 para Seguridad de la información*, enfocándose en el catalizador procesos (figura 84). Basándose en los requerimientos de los profesionales de seguridad de la información y el entorno operativo específico propio de la empresa, la empresa puede decidir si una fuente que contiene un determinado conjunto de guías particulares es relevante, y si la guía se aplica o pueden existir desfases.

Los siguientes estándares se incluyen en la comparación en este apéndice:

- Series ISO/IEC 27000 – La serie ISO/IEC 27000 proporciona un modelo para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI. Los siguientes dominios y áreas de *COBIT 5 para Seguridad de la información* se cubren en la serie ISO/IEC 27000, incluyendo los objetivos de control y controles del Anexo A de la ISO/IEC 27001:
  - Procesos de seguridad y relativos a riesgos de los dominios EDM, APO y DSS
  - Varias actividades referentes a seguridad dentro de procesos en otros dominios
  - Actividades de supervisión y evaluación del dominio MEA
- *ISF 2011 Standard of Good Practice for Information Security* se basa en el Modelo de Seguridad de la Información de ISF y consiste en un esquema general de buenas prácticas de negocio que se agrupan por áreas y se dividen en cuatro categorías principales: gobierno de seguridad de la información, requerimientos de seguridad de la información, marco de control y supervisión y mejora de la seguridad de la información.
- *Guide for Assessing the Information Security Controls in Federal Information Systems and Organisations*, NIST—El propósito de esta guía es proporcionar una orientación con respecto a los controles de seguridad de una agencia ejecutiva del gobierno de los EEUU. Este ejercicio usa la publicación especial NIST 800-53A Revisión 1.

Figura 84—Mapeo de *COBIT 5 para Seguridad de la Información* con Estándares Relacionados

COBIT 5 para Seguridad de la Información	ISO/IEC 27001	¿Relevante? ¿Aplicado?	ISO/IEC 27002	¿Relevante? ¿Aplicado?	ISF	¿Relevante? ¿Aplicado?	NIST	¿Relevante? ¿Aplicado?
EDM01 Asegurar el establecimiento y mantenimiento del marco de gobierno	5.1 Compromiso de la Dirección A.5 Política de Seguridad		6.1.1 Compromiso de la dirección con la seguridad de la información		SG1.1 Marco de Gobierno de la Seguridad			
EDM02 Asegurar la entrega de beneficiosy	7. Revisión de la gestión del SGSI 8. Mejora del SGSI				SG2.2 Entrega de Valor a los Interesados SG2.3 Programa de Aseguramiento de la Seguridad de la Información			
EDM03 Asegurar la optimización del riesgo	4.2.1 Construir el SGSI 4.2.2 Implementar y operar el SGSI 4.2.3 Supervisar y revisar el SGSI 4.3 Requisitos de documentación		14.1.2 Continuidad de negocio y gestión de riesgos		SR1 Evaluación de Riesgos de la Información CF20 Continuidad de Negocio SI2.2 Informes de Seguridad de la Información			
EDM04 Asegurar la optimización de los recursos	5.2 Gestión de recursos A.6 Organización de la seguridad de la información						Planificación	
EDM05 Asegurar la transparencia hacia las partes interesadas	A.10 Gestión de las comunicaciones y operaciones		6.1.1 Compromiso de la dirección con la seguridad de la información 6.1.2 Coordinación de la seguridad de la información 6.1.3 Establecimiento de responsabilidades de la seguridad de la información 6.1.4 Proceso de autorización de instalaciones para el tratamiento de la información 6.1.5 Acuerdos de confidencialidad 6.1.6 Contacto con autoridades 6.1.7 Contacto con grupos de interés especiales 6.1.8 Revisión independiente de la seguridad de la información		SG2.2 Entrega de Valor a los Interesados			
APO01 Gestionar la estrategia	5.1 Compromiso de la dirección A.5 Política de Seguridad A.6 Organización de la seguridad de la información		Organización de seguridad de la información		SG1.1 Marco de Gobierno de la Seguridad			
APO02 Gestionar la estrategia	4.2.1 Construir el SGSI				SG2.1 Estrategia de seguridad de la información			

Figura 84—Mapeo de *COBIT 5 para Seguridad de la Información* con Estándares Relacionados *(cont.)*

COBIT 5 para Seguridad de la Información	ISO/IEC 27001	¿Relevante? ¿Aplicado?	ISO/IEC 27002	¿Relevante? ¿Aplicado?	ISF	¿Relevante? ¿Aplicado?	NIST	¿Relevante? ¿Aplicado?
APO03 Gestionar la arquitectura empresarial					CF4 Aplicaciones de Negocio CF7 Gestión de Sistemas CF8 Infraestructura Técnica de Seguridad de la Información		Gestión de la Configuración	
APO04 Gestionar la innovación								
APO05 Gestionar el portafolio								
APO06 Gestionar el presupuesto y los costes								
APO07 Gestionar los recursos humanos	5.2.2 Formación, concienciación y competencia A.8 Seguridad ligada a los recursos humanos		Seguridad de la Información de Recursos Humanos		CF2 Seguridad de la Información de Recursos Humanos		• Concienciación y formación • Planificación • Seguridad de Información del Personal	
APO08 Gestionar las relaciones	A.6.1 Organización interna				CF5 Acceso de los Clientes			
APO09 Gestionar los acuerdos de servicio			10.2.1 Provisión de servicios 10.2.2 Supervisión y revisión de los servicios prestados por terceros 10.2.3 Gestión del cambio en los servicios prestados por terceros		CF7.7 Acuerdos de Nivel de Servicio SI2.1 Supervisión de la Seguridad SI2.2 Informes de Riesgos de la Información		Adquisición de Sistemas y Servicios	
APO10 Gestionar los proveedores	A.6.2 Terceros		6.1.5 Acuerdos de confidencialidad 6.2.1 Identificación de riesgos relacionados con terceros 6.2.3 Tratamiento de la seguridad en contratos con terceros 8.1.2 Investigación de antecedentes 8.1.3 Términos y condiciones de contratación 10.2.3 Gestión del cambio en los servicios prestados por terceros 10.8.2 Acuerdos de intercambio 12.4.2 Protección de datos de prueba del sistema 12.5.5 Externalización del desarrollo de software 15.1.4 Protección de datos y privacidad de la información de carácter personal		CF16 Gestión de Proveedores Externos		Adquisición de Sistemas y Servicios	

Figura 84—Mapeo de *COBIT 5 para Seguridad de la Información* con Estándares Relacionados *(cont.)*

COBIT 5 para Seguridad de la Información	ISO/IEC 27001	¿Relevante? ¿Aplicado?	ISO/IEC 27002	¿Relevante? ¿Aplicado?	ISF	¿Relevante? ¿Aplicado?	NIST	¿Relevante? ¿Aplicado?
APO11 Gestionar la calidad	7. Revisión de la gestión del SGSI 8. Mejora del SGSI				CF17.3 Aseguramiento de la Calidad			
APO12 Gestionar el riesgo	4.2.1 Construir el SGSI 4.2.2 Implementar y operar el SGSI 4.2.3 Supervisar y revisar el SGSI 4.3 Requisitos de documentación		13.1.1 Notificación de eventos de seguridad de la información 13.1.2 Notificación de puntos débiles de seguridad 14.1.1 Inclusión de seguridad de la información en el proceso de gestión de la continuidad del negocio 14.1.2 Continuidad del negocio y evaluación de riesgos		SR1 Evaluación de Riesgos de Información SR2 Cumplimiento CF1 Política y Organización de la Seguridad de la Información CF10 Gestión de Amenazas y Vulnerabilidades CF20 Continuidad del negocio SI2.2 Informes de Riesgos de la Información SI2.3 Supervisión del Cumplimiento de la Seguridad de la Información		• Respuesta a Incidentes • Evaluación de Riesgos	
APO13 Gestionar la seguridad	Tratado a lo largo de esta norma		Tratado a lo largo de esta norma		Tratado a lo largo de esta norma		Tratado a lo largo de esta norma	
BAI01 Gestionar los programas y proyectos							Gestión de Programas	
BAI02 Gestionar la definición de requisitos			10.1.1 Análisis y especificación de los requisitos de seguridad 10.3.2 Aceptación del sistema 11.6.2 Aislamiento de sistemas sensibles 12.1.1 Análisis y especificación de requisitos de seguridad		SR1.3 Requisitos de Confidencialidad SR1.4 Requisitos de Integridad SR1.5 Requisitos de Disponibilidad CF18.1 Especificación de Requisitos			
BAI03 Gestionar la Identificación y la construcción de soluciones	A.12 Adquisición, desarrollo y mantenimiento de sistemas de información		Tratado a lo largo de esta norma		CF17 Gestión del Desarrollo de Sistemas CF18 Ciclo de vida del Desarrollo de Sistemas		• Control de Acceso • Gestión de la Configuración • Mantenimiento • Adquisición de Sistemas y Servicios	
BAI04 Gestionar la disponibilidad y la capacidad			10.3.1 Gestión de la capacidad				• Planificación de contingencia • Planificación	
BAI05 Gestionar la introducción de cambios organizativos								
BAI06 Gestionar los cambios			10.1.2 Gestión de cambios 11.5.4 Uso de las utilidades del sistema 12.5.1 Procedimientos de control de cambios 12.5.3 Restricciones a los cambios en los paquetes de software 12.6.1 Control de las vulnerabilidades técnicas		CF7.6 Gestión de Cambios CF10 Gestión de Amenazas y Vulnerabilidades			

Figura 84—Mapeo de *COBIT 5 para Seguridad de la Información* con Estándares Relacionados *(cont.)*								
COBIT 5 para Seguridad de la Información	**ISO/IEC 27001**	**¿Relevante? ¿Aplicado?**	**ISO/IEC 27002**	**¿Relevante? ¿Aplicado?**	**ISF**	**¿Relevante? ¿Aplicado?**	**NIST**	**¿Relevante? ¿Aplicado?**
BAI07 Gestionar la aceptación del cambio y de la transición			6.1.4 Proceso de autorización de instalaciones para el tratamiento de la información 8.2.2 Concienciación, formación y capacitación en seguridad de la información 9.1.6 Áreas de acceso público y de carga y descarga 10.1.4 Separación de los recursos de desarrollo, prueba y operación 10.3.2 Aceptación del sistema 12.4.2 Protección de los datos de prueba del sistema 12.4.3 Control de acceso al código fuente de los programas 12.5.1 Procedimientos de control de cambios 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo		CF7.6 Change Management			
BAI08 Gestionar el conocimiento	4.3 Requisitos de documentación		10.1.1 Documentación de los procedimientos de operación 10.3.2 Aceptación del sistema 10.7.4 Seguridad de la documentación del sistema 13.2.2 Aprendizaje de los incidentes de seguridad de la información		CF3.2 Gestión Documental CF6 Gestión de Acceso		Control de Acceso	

Figura 84—Mapeo de *COBIT 5 para Seguridad de la Información* con Estándares Relacionados *(cont.)*

COBIT 5 para Seguridad de la Información	ISO/IEC 27001	¿Relevante? ¿Aplicado?	ISO/IEC 27002	¿Relevante? ¿Aplicado?	ISF	¿Relevante? ¿Aplicado?	NIST	¿Relevante? ¿Aplicado?
BAI09 Gestionar los activos	A.7 Gestión de activos		7.1.1 Inventario de activos 7.1.2 Propiedad de los activos 7.2.2 Etiquetado y manipulado de la información 10.7.4 Seguridad de la documentación del sistema 11.4.3 Identificación de los equipos en las redes 12.4.1 Control del software en explotación 12.4.2 Protección de los datos de prueba del sistema 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo 12.5.3 Restricciones a los cambios en los paquetes de software 12.6.1 Control de las vulnerabilidades técnicas 15.1.5 Prevención del uso indebido de los recursos de tratamiento de la información		CF3 Gestión de activos CF19 Seguridad Física y Ambiental de la Información		• Protección de medios • Protección física y ambiental	
BAI10 Gestionar la configuración			7.1.1 Inventario de activos 7.1.2 Propiedad de los activos 7.2.2 Etiquetado y manipulado de la información 10.7.4 Seguridad de la documentación del sistema 11.4.3 Identificación de los equipos en las redes 12.4.1 Control del software en explotación 12.4.2 Protección de los datos de prueba del sistema 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo 12.5.3 Restricciones a los cambios en los paquetes de software 12.6.1 Control de las vulnerabilidades técnicas 15.1.5 Prevención del uso indebido de los recursos de tratamiento de la información		CF4 Aplicaciones de Negocio CF6 Gestión de Acceso CF7 Gestión de Sistemas CF8 Infraestructura Técnica de Seguridad de la Información CF9 Gestión de Red CF12 Entornos Locales CF13 Aplicaciones de Escritorio CF14 Informática Móvil CF15 Comunicaciones Electrónicas		• Control de Acceso • Gestión de la Configuración • Adquisición de Sistemas y Servicios	

Figura 84—Mapeo de *COBIT 5 para Seguridad de la Información* con Estándares Relacionados *(cont.)*

COBIT 5 para Seguridad de la Información	ISO/IEC 27001	¿Relevante? ¿Aplicado?	ISO/IEC 27002	¿Relevante? ¿Aplicado?	ISF	¿Relevante? ¿Aplicado?	NIST	¿Relevante? ¿Aplicado?
DSS01 Gestionar las operaciones	4.2.2 Implementar y operar el SGSI		Gestión de comunicaciones y operaciones		CF6 Gestión de Acceso CF7 Gestión de Sistemas CF9 Gestión de Red			
DSS02 Gestionar las peticiones y los incidentes del servicio	A.13 Gestión de incidentes de seguridad de la información		Gestión de incidentes de seguridad de la información		CF10 Gestión de Amenazas y Vulnerabilidades CF11 Gestión de incidentes		Respuesta a Incidentes	
DSS03 Gestionar los problemas			13.2.2 Aprendizaje de los incidentes de seguridad de la información		CF10 Gestión de Amenazas y Vulnerabilidades CF11 Gestión de Incidentes		Respuesta a Incidentes	
DSS04 Gestionar la continuidad	4.2.4 Mantener y mejorar el SGSI 4.3 Requisitos de documentación 8. Mejora del SGSI A.14 Gestión de la continuidad del negocio		Gestión de la continuidad del negocio		CF20 Continuidad del Negocio		Planificación de contingencias	
DSS05 Gestionar los servicios de seguridad	Tratado a lo largo de esta norma		Tratado a lo largo de esta norma		Tratado a lo largo de esta norma		Tratado a lo largo de esta norma	
DSS06 Gestionar los controles de los procesos del negocio	4.2.3 Supervisar y revisar el SGSI		8.2.1 Responsabilidades de la dirección 10.1.3 Segregación de tareas 10.1.4 Separación de los recursos de desarrollo, prueba y operación 10.5.1 Copias de seguridad de la información 10.6.1 Controles de red 10.7.3 Procedimientos de manipulación de la información 10.8.3 Soportes físicos en tránsito 10.8.4 Mensajería electrónica 12.4.2 Protección de los datos de prueba del sistema 12.4.3 Control de acceso al código fuente de los programas		CF1 Política y Organización de la Seguridad de la Información CF7 Gestión de Sistemas		• Protección de medios • Integridad de Sistemas e Información	
MEA01 Supervisar, evaluar y valorar rendimiento y conformidad	4.2.3 Supervisar y revisar el SGSI 4.2.4 Mantener y mejorar el SGSI 7. Revisión de la gestión del SGSI		10.10.2 Supervisión del uso del sistema 5.1.2 Revisión de la política de seguridad de la información 6.1.8 Revisión independiente de la seguridad de la información 10.10.2 Supervisión del uso del sistema		SR2 Cumplimiento SI1 Auditoría de la Seguridad de la Información SI2 Rendimiento de la Seguridad de la Información		• Auditoría y Responsabilidad • Autorización y Evaluación de la Seguridad de la Informaciónn	

Figura 84—Mapeo de *COBIT 5 para Seguridad de la Información* con Estándares Relacionados *(cont.)*

COBIT 5 para Seguridad de la Información	ISO/IEC 27001	¿Relevante? ¿Aplicado?	ISO/IEC 27002	¿Relevante? ¿Aplicado?	ISF	¿Relevante? ¿Aplicado?	NIST	¿Relevante? ¿Aplicado?
MEA02 Supervisar, evaluar y valorar el sistema de control interno	4.2.3 Supervisar y revisar el SGSI 6. Auditoría interna del SGSI A.15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico		5.1.1 Documento de política de seguridad de la información 5.1.2 Revisión de la política de seguridad de la información 6.1.8 Revisión independiente de la seguridad de la información 6.2.3 Tratamiento de la seguridad en contratos con terceros 10.2.2 Supervisión y revisión de los servicios prestados por terceros 10.10.2 Supervisión del uso del sistema 10.10.4 Registros de administración y operación 15.2.1 Cumplimiento de políticas y normas de seguridad 15.2.2 Comprobación del cumplimiento técnico 15.3.1 Controles de auditoría de los sistemas de información		CF1 Política y Organización de la Seguridad de la Información SI1 Auditoría de la Seguridad de la Información		Auditoría y Responsabilidad	
MEA03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos	6. Auditoría interna del SGSI A.15.1 Cumplimiento de los requisitos legales A.15.3 Consideraciones sobre la auditoría de los sistemas de información		6.1.6 Contacto con las autoridades 15.1.1 Identificación de la legislación aplicable 15.1.2 Derechos de propiedad intelectual (IPR) 15.1.4 Protección de datos y privacidad de la información de carácter personal		SR2 Cumplimiento			

Acrónimos

Término	Definición
CCTV	Circuito cerrado de televisión televisión (Closed-circuit television)
CGEIT	Certificado en Gobierno Corporativo de las Tecnologías de la Información Información (Certified in the Governance of Enterprise IT)
CIA	Confidencialidad, integridad y disponibilidad (Confidentiality, integrity and availability)
CISA	Certificado en Auditoría de los Sistemas de Información (Certified Information Systems Auditor)
CISM	Certificado en Gestión de los Sistemas de Información (Certified Information Security Manager)
CISSP	Certificado de Profesional de Seguridad en Sistemas de Información (Certified Information System Security Professional)
CMDB	Base de datos de gestión de la configuración (Configuration management data base)
CRISC	Certificado en Sistemas de Información de Riesgos y Control (Certified in Risk and Information Systems Control)
CRL	CRL Lista de certificados revocados (Certificate revocation list)
DLP	Prevención de pérdida de datos (Data loss prevention or data leak prevention)
DPI	Inspección profunda de paquetes (Deep packet inspection)
ERM	Gestión general de riesgos corporativos (Enterprise risk management)
FTP	Protocolo de transferencia de archivos (File Transfer Protocol)
IDaaS	IDaaS Identidad como Servicio (Identity as a Service)
NIST	Instituto Nacional de Estándares y Técnología, EE.UU. (National Institute of Standards and Technology)
NOC	Centro de Operaciones de Red (Network operations center)
OMA DM	Gestión de dispositivos de la Alianza Móvil Abierta (Open Mobile Alliance Device Management)
OSS	Software de código abierto (Open source software)
OTP	Contraseña de un solo uso (One-time password)
PCI DSS	Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (Payment Card Industry Data Security Standards)
PKI	Infraestructura de lave pública (Public key infrastructure)
PMO	Oficina de gestión de proyectos (Project management office)
SIEM	Gestión de la información y los eventos de seguridad (Security information and event management)
SIM	Módulo de identidad de suscriptor (Subscriber identity module)
SNMP	Protocolo Simple de Gestión de Red (Simple Network Management Protocol)
UPC	Código universal de producto (Universal product code)
VPN	Red privada virtual (Virtual private network)

Página dejada en blanco intencionadamente

GLOSARIO

Término	Definición
Actividad	En COBIT, la acción principal tomada para operar el proceso. Directrices para alcanzar prácticas de gestión para un gobierno y gestión de TI exitoso en la empresa. Actividades: • Describe un conjunto de tareas orientadas a la acción necesarios y suficientes para alcanzar una Práctica de Gobierno o una Práctica de Gestión. • Considerar las entradas y salidas del proceso. • Se basan en estándares y buenas prácticas aceptados de forma generalizada. • Apoyan el establecimiento de roles y responsabilidades claros. • No son prescriptivas y deben adaptarse y desarrollarse en procedimientos apropiados para la empresa.
Alineamiento	Un estado en el que los elementos facilitadores del gobierno y la gestión de TI de la empresa contribuyen a las metas y las estrategias de la misma.
Autenticación	El acto de verificar la identidad de un usuario y sus derechos de acceso a información en los sistemas. Nota del alcance: Seguridad: La autenticación está diseñada para proteger frente a una actividad de inicio de sesión fraudulenta. Se puede referir también a la verificación de lo correcto de una pieza de información.
Buena práctica	Actividad o proceso probado que ha sido usado con éxito por múltiples empresas y ha demostrado que produce resultados fiables.
Calidad	Ser adecuado al propósito (alcanzar el valor esperado).
Certificación (general)	Una evaluación independiente declarando que un producto, persona, proceso o sistema de gestión cumplen unos requerimientos específicos.
Comité de Arquitectura	Un grupo de partes interesadas y expertos que son responsables de guiar a la empresa en aspectos y decisiones relacionados con la arquitectura de empresa y de establecer las políticas y normas de arquitectura.
Competencia	La habilidad de realizar una tarea, acción o función específicas con éxito.
Confidencialidad	Preservar las restricciones autorizadas en el acceso y la revelación, incluyendo los medios para proteger la privacidad y la información propietaria.
Contexto	El conjunto completo de factores internos y externos que pueden influir o determinar como actúa una empresa, entidad, proceso o individuo. Nota de alcance: El contexto incluye: • Contexto tecnológico—Factores tecnológicos que afectan la capacidad de una organización para extraer valor de los datos. • Contexto de datos—La precisión de los datos, su disponibilidad, grado de actualización y calidad. • Habilidades y conocimiento—Experiencia general y habilidades analíticas, técnicas y de negocio. • Contexto organizativo y cultural—Factores políticos, y si la organización prefiere datos a la intuición. • Contexto estratégico—Metas corporativas estratégicas.
Continuidad de negocio	Evitar, mitigar y recuperarse de una interrupción. Se puede usar en este contexto también los términos “planificación de la restauración del negocio”, “planificación para recuperación de desastres” y “planificación de las contingencias”; se enfocan en los aspectos de la recuperación dentro de la continuidad y, por esa razón, el factor “resiliencia” también debería ser considerado.
Control	Los medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden tener una naturaleza administrativa, técnica, de gestión, o legal. También usada como sinónimo de salvaguarda o contramedida.
Control de procesos de negocio	Las políticas, procedimientos, prácticas y estructuras organizativas diseñadas para generar garantías de que un proceso de negocio conseguirá sus objetivos.
Creación de valor	El objetivo principal del gobierno de una empresa, conseguido cuando los tres objetivos subyacentes (consecución de beneficios, optimización de riesgo y optimización de recursos) están en equilibrio.
Cultura	Un patrón de comportamientos, creencias, hipótesis, actitudes y formas de hacer las cosas.
Disponibilidad	Asegurar un acceso y un uso a tiempo y fiable de la información.
Dispositivo de claves	Dispositivo de acceso seguro a la información con autenticación incorporada que se utiliza para controlar y asegurar el acceso.
Entradas y salidas	Los elementos/productos del trabajo en un proceso que se consideran necesarios para soportar la operación de un proceso. Son los que posibilitan la toma de decisiones clave, proveen un registro y traza de auditoria de las actividades del proceso y posibilitan el seguimiento en caso de un incidente. Se definen al nivel de práctica de gestión clave y pueden incluir algunos productos de trabajo usados únicamente dentro del proceso y son, comúnmente, entradas esenciales para otros procesos. Las entradas y salidas de COBIT 5 son ilustrativas y no deben considerarse como una lista exhaustiva ya que se pueden definir flujos de información adicionales dependiendo del entorno particular de una empresa y de su marco de procesos
Estructura organizativa	Un catalizador del gobierno y de la gestión. Incluye la empresa y sus estructuras, jerarquías y dependencias. Ejemplo: Comité de Seguimiento.

Término	Definición
Facilitador de gobierno	Algo (tangible o intangible) que ayuda a la realización de un gobierno efectivo.
Gestión	La gestión planifica, construye, ejecuta y supervisa actividades alineadas con la dirección establecida por el órgano de gobierno para alcanzar los objetivos de la empresa.
Gestión de riesgos	Uno de los objetivos de gobierno. Requiere reconocer un riesgo; evaluar su impacto y probabilidad; y desarrollar estrategias, como, por ejemplo, evitar el riesgo, reduciendo el efecto negativo de riesgo y/o transfiriendo el riesgo, para gestionarlo en el contexto del apetito de riesgo de una empresa.
Gobierno	El gobierno asegura que las necesidades, condiciones y opciones de los grupos de interés han sido evaluadas para determinar unos objetivos a alcanzar equilibrados y acordados; establecer la dirección mediante la priorización y la toma de decisiones; y monitorización del rendimiento y el cumplimiento de la dirección y objetivos acordados.
Gobierno de la empresa	Un conjunto de responsabilidades y prácticas ejercidas por el Consejo de Administración y los gestores ejecutivos con el objetivo de dotar de dirección estratégica, asegurando que los objetivos son conseguidos, verificando que el riesgo es gestionado de forma apropiada y verificando que los recursos de la empresa son usados de forma responsable. También podría referirse a una visión de gobierno que ve el conjunto de la empresa; la visión más alta de gobierno con la que todas las demás deben alinearse.
Gobierno de TI empresarial	Un enfoque de gobierno que garantiza que las tecnologías de información y las relacionadas soportan y habilitan la estrategia de la empresa y la consecución de las metas corporativas. También incluye el gobierno funcional de TI, por ejemplo, garantizando que las capacidades de TI son provistas de forma eficiente y efectiva.
Habilidad	La capacidad aprendida de conseguir ciertos resultados predeterminados.
Honeypot (sistema cebo)	Servidor especialmente configurado, también conocido como servidor señuelo, diseñado para atraer y monitorizar intrusos de forma que sus acciones no afecten a los sistemas en producción.
Información	Un activo que, como cualquier otro activo importante de negocio, es esencial para el negocio de una empresa. Puede existir de muchas formas: impreso o escrito en papel, almacenado electrónicamente, transmitido por correo o de forma electrónica, mostrado en películas o hablado durante una conversación.
Instrumento de prueba	Entorno o sistema que proporciona la capacidad de realizar pruebas contra una entidad con un conjunto de resultados esperados.
Integridad	Proteger contra una modificación o destrucción impropia de información, e incluye asegurar el no repudio y la autenticidad de la información.
Marco de gobierno	Un marco es una estructura conceptual básica usada para resolver y responder a temas complejos; un facilitador de gobierno; un conjunto de conceptos, hipótesis y prácticas que definen como se puede afrontar o entender algo, las relaciones entre las entidades involucradas, los roles de aquellos involucrados y las fronteras (qué está y qué no está incluido en el sistema de gobierno). Ejemplos: COBIT y Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) Internal Control—Integrated Framework.
Meta de empresa	Vea objetivo de negocio
Modelo	Un modo de describir un conjunto de componentes y de como esos componentes se relacionan entre ellos para describir el funcionamiento principal de un objeto, sistema o concepto.
Motivación	Factores externos e internos que inician y afectan cómo una empresa o individuos actúan o cambian.
Objetivo	Declaración de un resultado deseado.
Objetivo de negocio	La traducción de la misión de la empresa desde una expresión de intenciones a unas metas de rendimiento y resultados.
Oficina de gestión de programas y proyectos (PMO)	La función responsable de dar apoyo a los gestores de programa y de proyecto, y de reunir, evaluar y reportar información sobre el estado de los programas y proyectos constitutivos de los mismos.
Optimización de recursos	Uno de los objetivos del gobierno. Incluye un uso efectivo, eficiente y responsable de todos los recursos--humanos, financieros, equipamiento, inmuebles, etc.
Parte consultada (RACI)	Se refiere a aquellas personas cuyas opiniones son buscadas en una actividad (comunicación bidireccional). En una matriz RACI responde a la pregunta: **¿Quién proporciona las entradas?** Roles claves que proporcionan entradas. Hay que subrayar que los roles responsables de ejecutar la tarea y los que son responsables de que se haga también deben obtener la información de otras unidades o de socios externos; sin embargo, deben considerarse las entradas de los roles listados y, si se requiere, se debe tomar una acción adecuada para su escalado, incluyendo la información del dueño del proceso y/o del comité de supervisión.
Parte informada (RACI)	Se refiere a aquellas personas que son actualizadas con el progreso de una actividad (comunicación unidireccional). En una matriz RACI responde a la pregunta: **¿Quién recibe información?** Los roles que son informados de la consecución de metas y/o los entregables de la tarea. El rol 'responsable de que se haga' por supuesto debería siempre recibir información apropiada para supervisar la tarea, al igual que otros roles responsables para cada una de sus áreas de interés.
Parte interesada	Cualquiera que tiene una responsabilidad, expectativa o cualquier otro interés en la empresa –por ejemplo, accionistas, usuarios, el gobierno, proveedores, clientes y el publico en general.

Término	Definición
Parte responsable (RACI)	Se refiere a la persona encargada de conseguir que las actividades se completen satisfactoriamente.
En una matriz RACI responde a la pregunta: ¿Quién está ejecutando la tarea?	A statement describing the desired outcome of a process. An outcome can be an artefact, a significant change of a state or a significant capability improvement of other processes. En una matriz RACI responde a la pregunta: **¿Quién está ejecutando la tarea?** Roles que toman la responsabilidad operacional principal en completar la tarea listada y en generar el resultado deseado.
Parte responsable de que se haga / (aprobadora) – RACI	El individuo, grupo o entidad que tiene la responsabilidad última sobre una materia, proceso o alcance. En una matriz RACI responde a la pregunta: **¿A quién hay que pedir cuentas por el éxito de la tarea?**
Política	Intención y dirección global según se expresa formalmente por los gestores.
Práctica de gobierno / gestión	Para cada proceso COBIT, las prácticas de gobierno y gestión proveen un conjunto completo de requerimientos de alto nivel para el gobierno y la gestión efectiva y práctica de TI de una empresa. Se trata de declaraciones de acción de los cuerpos de gobierno y gestión.
Principio	Un catalizador del gobierno y la gestión. Comprende los valores y las hipótesis fundamentales contenidas en la empresa, las creencias que la guían y que definen sus límites entorno a los procesos de decisión, comunicación interna o externa y la administración--cuidado de los activos que pertenecen a otros.
Proceso	Generalmente, una colección de prácticas influenciadas por las políticas y procedimientos de la empresa que toma entradas de una serie de fuentes (incluyendo otros procesos), manipula esas entradas y genera salidas (por ejemplo, productos, servicios). Nota de alcance: Los procesos tienen claras razones de negocio para su existencia, dueños responsables de su realización, roles claros y adscripción de responsabilidades alrededor de la ejecución del proceso y medios para medir su rendimiento
Propietario	Individuo o grupo que sustenta o posee los derechos de y las responsabilidades para una empresa, entidad o activo, por ejemplo, un propietario de negocio, un propietario de un sistema.
Pruebas de aproximación	Software que realiza una técnica de análisis de vulnerabilidad, a menudo automática o semi-automática, que implica proporcionar datos inválidos, inesperados o aleatorios a las entradas de un programa o sistema informático. Las vulnerabilidades identificadas esta técnica pueden llevar al compromiso del sistema.
Realización de beneficios	Uno de los objetivos del gobierno. La generación de nuevos beneficios para la empresa, el mantenimiento y ampliación de las formas existentes de beneficios y la eliminación de aquellas iniciativas y activos que no están creando suficiente valor.
Recurso	Cualquier activo de la empresa que puede ayudar a la organización a conseguir sus objetivos.
Riesgo	La combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 73).
Rol	Comportamiento prescrito o esperado asociado con una posición o estatus particular en un grupo u organización. Un trabajo o puesto que tiene un conjunto de expectativas específicas unidas al mismo.
Salida	Ver Entradas y salidas
Seguridad de la información	Asegura que dentro de la empresa, la información es protegida frente a revelaciones a usuarios no autorizados (confidencialidad), modificación inadecuada (integridad) e imposibilidad de acceso cuando se necesita (disponibilidad).
Servicio TI	La provisión diaria a clientes de la infraestructura y de las aplicaciones TI y del soporte para su uso. Los ejemplos incluyen el centro de servicios, la provisión de equipamiento y los movimientos, y las autorizaciones de seguridad.
Servicios	Vea Servicio TI.
Sniffer	También conocido como paquete analizador, analizador de red o analizador de protocolo. Software o hardware que puede interceptar y registrar el tráfico que pasa por una red digital.
Tarpit	Servicio o sistema informático (normalmente un servidor) que retrasa las conexiones entrantes tanto como le es posible. Desarrollado como una defensa contra gusanos informáticos, con la idea de que los abusos sobre las redes tales como el correo basura o los escaneos masivos son menos efectivos si llevan demasiado tiempo.

Página dejada en blanco intencionadamente